Hotwire® Management Communications Controller (MCC) Card

IP Conservative

User's Guide

Document No. 8000-A2-GB22-80

September 2003

PARADYNE®

Copyright © 2003 Paradyne Corporation.
All rights reserved.
Printed in U.S.A.

Notice

This publication is protected by federal copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission of Paradyne Corporation, 8545 126th Avenue North, P.O. Box 2826, Largo, Florida 33779-2826.

Paradyne Corporation makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Further, Paradyne Corporation reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Paradyne Corporation to notify any person of such revision or changes.

Changes and enhancements to the product and to the information herein will be documented and issued as a new release to this manual.

Warranty, Sales, Service, and Training Information

Contact your local sales representative, service representative, or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training, distributor locations, or Paradyne worldwide office locations, use one of the following methods:

- **Internet:** Visit the Paradyne World Wide Web site at **www.paradyne.com**. (Be sure to register your warranty at **www.paradyne.com/warranty**.)
- **Telephone:** Call our automated system to receive current information by fax or to speak with a company representative.
  - — Within the U.S.A., call 1-800-870-2221
  - — Outside the U.S.A., call 1-727-530-2340

Trademarks

ACCULINK, COMSPHERE, FrameSaver, Hotwire, MVL, NextEDGE, OpenLane, and Performance Wizard are registered trademarks of Paradyne Corporation. ReachDSL and TruePut are trademarks of Paradyne Corporation. All other products and services mentioned herein are the trademarks, service marks, registered trademarks, or registered service marks of their respective owners.

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773, or send e-mail to **userdoc@paradyne.com**. Include the number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

Contents

About This Guide

- Document Purpose and Intended Audience vii
- New Features for this Release viii
- Document Summary viii
- Product-Related Documents ix

1 About the MCC Card

- Overview 1-1
- Features 1-3
- Levels of Access 1-4
- Software Functionality 1-5
  - The MCC Configuration Menu 1-5
  - The MCC Monitoring Menu 1-6
  - The MCC Applications Menu 1-6
  - The MCC Diagnostics Menu 1-6

2 Menus and Screens

- User Interface Formats 2-1
  - Menu Components 2-1
  - Screen Components 2-2
- Navigation Keys 2-3
- Accessing the System 2-4
  - User Login Screen 2-4
- Hotwire Menu Structure 2-5
  - Hotwire Chassis Main Menu 2-5
  - Quick Card Select Screen 2-6
  - Port Card Select Screen 2-6
  - Mgmt. Card Select Screen 2-6
  - Managed SN Select Screen 2-6
  - Accessing a Selection Screen 2-7
  - Hotwire – MCC Menu 2-10
  - Configuration Menu 2-11
  - Monitoring Menu 2-12
  - Applications Menu 2-12

Diagnostics Menu 2-12
Chassis Information Screen. 2-13
Current Users Screen 2-13
- Exiting the System 2-14
Manually Logging Out 2-14
Automatically Logging Off 2-14

3 Setup and Configuration

- Overview 3-1
- Interface Naming Convention. 3-1
- Domain Types 3-2
Service Domain 3-2
Management Domain 3-2
Management Domain Components. 3-3
- Accessing the System for the First Time 3-4
- Management Domain Configuration 3-6
Task 1: Creating the Default Route 3-6
Task 2: Creating SNMP Community Strings and Enabling Authentication Failure Traps 3-7

4 Configuration Menu Options

- Overview 4-1
- Configuration Menu Overview 4-2
- Card Status Menu 4-3
Entering Card Information 4-4
Configuring Access to DNS Servers 4-4
Setting the Time and Date. 4-5
Clearing NVRAM 4-5
Uploading/Downloading Configuration Data from a TFTP Server (NVRAM Config Loader). 4-6
Resetting the MCC Card 4-7
Downloading Code 4-8
Card Status Menu Options 4-8
- Ports Menu 4-13
- Interfaces Menu 4-14
Obtaining General Interface Information and Changing MTU Value 4-15
Configuring IP Addresses for the e1a Port 4-16
Stopping, Starting, and Monitoring an Interface 4-17
Interfaces Menu Options 4-18

- Access Security Menu 4-19
  - Adding, Changing, and Deleting Users 4-19
  - Enabling and Disabling RADIUS Authentication 4-21
  - Enabling and Disabling Telnet, FTP, and SNMP Access 4-22
  - Access Security Menu Options 4-24
- IP Router Menu 4-26
  - Adding and Deleting Static Routes 4-27
  - Adding and Deleting Martian Networks 4-28
  - Adding, Changing, and Deleting Filters 4-29
  - Using the ARP Submenu Options 4-31
  - Mapping IP Addresses and Host Names 4-32
- SNMP Menu 4-36
  - Defining a Community and Enabling Traps 4-36
  - SNMP Menu Options 4-38
- Slot (DSL Cards) Menu 4-39
  - Resetting a Slot 4-40
  - Configuring the IDSL Clock 4-41
  - Slot (DSL Cards) Menu Options 4-42
- SYSLOG Menu 4-44
- Files Menu 4-45
  - Configuring Automatic Backup of Card Configuration and Resynchronization of Backup Files 4-46

5 Monitoring Menu Options

- Overview 5-1
- Card Status Menu Options 5-2
  - Displaying General Card Information 5-3
  - Displaying Login History 5-4
  - Displaying System Errors 5-5
- Physical Layer Menu Options 5-6
  - Displaying Active Ports 5-7
  - Displaying Ethernet Statistics 5-8
- Interfaces Menu Options 5-10
  - Displaying Active Interfaces 5-11
  - Displaying Additional Interface Status 5-12
- Network Protocol Menu Options 5-13
  - Displaying Socket Statistics 5-14
  - Displaying UDP Statistics 5-16
  - Displaying TCP Statistics 5-17
  - Displaying TCP Connection Statistics 5-19
  - Displaying IP Statistics 5-20

Displaying ICMP Statistics 5-21
Displaying SNMP Statistics 5-22
Displaying SNMP Authentication Statistics 5-24
- IP Router Menu Options 5-25
Displaying Routing Table Information and Statistics 5-26
Displaying ARP Table Information 5-28
Displaying Filters 5-29
- Servers Menu Options 5-30
- Files Menu Options 5-32

6 Applications Menu Options

- Overview 6-1
Ping 6-2
TraceRoute 6-3
Telnet 6-4

7 Diagnostics Menu Options

- Overview 7-1
Selftest 7-2
Alarm 7-3

8 Troubleshooting

- Troubleshooting the DSL System 8-1
Accessing the DSL Cards and Service Nodes (SNs) 8-2
- Alarms 8-2
Major Alarms 8-3
Minor Alarms 8-4
- Management Domain Problems 8-5
High-Level Troubleshooting 8-5
MCC Card Cannot Ping Next Hop Router 8-6
MCC Cannot Ping NMS Server 8-7
Performance Issues – Viewing Network Statistics 8-8
Recovering from a Failed Download 8-8
Recovering from a Failed Login Attempt 8-8

A Upgrade Procedures

- Upgrade Instructions Overview A-1
- Firmware Download Sequence A-2
  - For All Cards (Except ReachDSL) A-2
  - For ReachDSL Cards A-2
- Accessing Firmware/Software Files A-3
- Firmware Version Numbers A-3
- Firmware Upgrade Procedures A-4
  - Manual Firmware Download A-5
  - Downloading New Firmware A-5
  - MCP Flash File System A-7
  - Uploading Files to the MCP's FFS. A-8
  - Verifying Firmware Upload to the MCP's FFS A-9
  - Saving a Card Configuration A-11
  - Saving MCC Card Configurations to a Host Computer (PC) A-12
  - Automatic Firmware Download A-12
  - Downloading Firmware in slot_n Directory A-13
  - Download Examples A-14

B IP Filtering Overview and Worksheets

- Overview B-1
- What is a Filter? B-1
- IP Filtering Configuration Worksheets B-3
  - Summary: How to Define a Filter B-3
  - Worksheet: Defining the Filter and Rules B-3
  - Worksheet: Binding the Filter. B-7

C Input Screens

- MCC Card Input Screens C-1

D Remote Access

- Accessing the MCC Card through a Modem D-1

E Simple Network Management Protocol

- SNMP Overview E-1
  - Community Structures E-2
- SNMP Gets and Sets E-3
  - Settable Objects E-3

- Traps E-4
  - MCC Traps E-4
  - DSL Traps E-5
  - authenticationFailure Trap E-7
- IP Conservation E-8
- Management Domain Packet Walk-Through E-8
  - SNMP to the MCC card E-8
  - SNMP to a DSL Card (AN) E-9
- Supported MIBs E-9
  - Standard MIBs E-9
  - System Group E-10
  - Interfaces Group E-10
  - Extension to the Interface Table E-10
  - IP Group E-10
  - ICMP Group, MIB II E-10
  - UDP Group, MIB II E-10
  - Transmission Group, MIB II E-10
  - SNMP Group, MIB II E-10
  - Ethernet Interface MIB E-11
  - Entity MIB E-11
- Paradyne Enterprise MIBs E-11
- Network Management Components E-13
- OpenLane Network Management Systems Overview E-15
  - Features of OpenLane E-15
- SNMP Configuration Worksheets E-16
  - Summary: Configuring the SNMP Agent E-16
  - Worksheet: Defining a Community and Enabling Traps E-17
  - Worksheet: Preventing Unauthorized Access E-20

Index

About This Guide

Document Purpose and Intended Audience

This guide describes how to configure the Management Communications Controller (MCC) card, troubleshoot, and operate the software component of the MCC card. The MCC, MCP, or MCC Plus card is a single resource in the Hotwire® Digital Subscriber Line Access Multiplexer (DSLAM) or GranDSLAM chassis that provides consolidated management access for Hotwire Digital Subscriber Line (DSL) cards such as Rate Adaptive DSL (RADSL) cards, ReachDSL™ cards, ISDN DSL (IDSL cards), Packet Symmetric Digital Subscriber Line (SDSL) cards, Asynchronous Transfer Mode (ATM) cards, and Time Division Multiplexer (TDM) SDSL cards, TDM Symmetric High-bit-rate Digital Subscriber Line (SHDSL) cards, as well as for the customer premises endpoints known as Service Nodes (SNs).

Use this guide to:

- Obtain a basic understanding of the MCC card's functionality
- Understand how to configure, monitor, and troubleshoot the MCC card

This guide is intended for administrators and operators who maintain the networks that support Hotwire network operations. A basic understanding of internetworking protocols and their features is assumed. Specifically, you should have familiarity with Simple Network Management Protocol (SNMP), Network Management Systems (NMSs), and the following internetworking concepts:

- TCP/IP applications
- IP and subnet addressing
- IP routing (also referred to as IP forwarding)

It is assumed that you have already installed either the Hotwire 8600/8610, 8800/8810 DSLAM or 8620/8820 GranDSLAM, and the appropriate MCC card. If you have not done so already, refer to the appropriate Hotwire chassis installation guide for installation instructions.

NOTE:

You should use this document in conjunction with the appropriate DSL Card User's Guide. These documents provide information about specific DSL cards you have installed in the Hotwire chassis. See *Product-Related Documents*.

New Features for this Release

MCP card Model Number 8900-B1-211 was created to reside in the same DSLAM as a Shelf Concentration and Processing (SCP) card, permitting management of all line card types.

Document Summary

Section	Description
Chapter 1, *About the MCC Card*	Provides an overview of the features and functionality of the Hotwire MCC card.
Chapter 2, *Menus and Screens*	Provides an overview of the menus and screens used by the Hotwire MCC card.
Chapter 3, *Setup and Configuration*	Provides step-by-step instructions on accessing the system for the first time. Also contains instructions on initial configuration of your Hotwire DSL system.
Chapter 4, *Configuration Menu Options*	Provides step-by-step instructions for each option on the Configuration Menu. Use these options to customize the MCC card.
Chapter 5, *Monitoring Menu Options*	Provides step-by-step instructions for each option on the Monitoring Menu. Use these options to monitor the MCC card.
Chapter 6, *Applications Menu Options*	Provides step-by-step instructions for each option on the Applications Menu. Use these options to perform Ping, TraceRoute and Telnet applications.
Chapter 7, *Diagnostics Menu Options*	Provides step-by-step instructions for each option on the Diagnostics Menu. Use these options to perform diagnostic functions.
Chapter 8, *Troubleshooting*	Describes Hotwire troubleshooting solutions.
Appendix A, *Upgrade Procedures*	Provides firmware upgrade procedures.
Appendix B, *IP Filtering Overview and Worksheets*	Provides an overview of MCC IP filters and worksheets to help you plan filter configuration on your network.
Appendix C, *Input Screens*	Provides an alphabetical list of all MCC input screens and the menu selection sequence required to reach each screen.
Appendix D, *Remote Access*	Summarizes guidelines for accessing the MCC through a dial-in modem.
Appendix E, *Simple Network Management Protocol*	Summarizes how SNMP is used with the MCC.
Index	Lists key terms, acronyms, concepts, and sections in alphabetical order.

Product-Related Documents

Document Number	Document Title
5620-A2-GN11	*Hotwire 5620 RTU Installation Instructions*
6301-A2-GN10	*Hotwire 6301/6302 IDSL Routers Installation Instructions*
6310-A2-GN12	*Hotwire 6310 ReachDSL v1 (MVL) Modem, Model 6310-A4, with Inline Phone Filter, Installation Instructions*
6341-A2-GN10	*Hotwire 6341/6342 SDSL Routers Installation Instructions*
6350-A2-GN12	*Hotwire 6350 ReachDSL Modem, Model 6350-A4, with Inline Phone Filter, Installation Instructions*
6351-A2-GN10	*Hotwire 6351 ReachDSL Router Installation Instructions*
6371-A2-GB20	*Hotwire DSL Routers User's Guide*
6371-A2-GN10	*Hotwire 6371 RADSL Router Installation Instructions*
7800-A2-GB31	*OpenLane SLM Administrator's Guide*
7900-A2-GB21	*Hotwire TDM SDSL Standalone Termination Units, Models 7974-A2, 7975-A2, and 7976-A2, User's Guide*
7970-A2-GB20	*Hotwire TDM SDSL Standalone Termination Units, Models 7974-A1, 7975-A1, 7976-A1, 7984-A1, 7985-A1, and 7986-A1, User's Guide*
8000-A2-GB26	*Hotwire MVL, ReachDSL, RADSL, IDSL, and SDSL Cards, Models 8310, 8312/8314, 8510/8373/8374, 8303/8304, and 8343/8344, User's Guide*
8000-A2-GZ40	*Hotwire MCC Card, IP Conservative, Installation Instructions*
8021-A2-GB20	*Hotwire Shelf Concentration Module (SCM) Card User's Guide*
8021-A2-GZ40	*Hotwire Shelf Concentration Module (SCM) Card Installation Instructions*
8303-A2-GZ40	*Hotwire 8303/8304 IDSL Cards Installation Instructions*
8310-A2-GZ40	*Hotwire 8310 MVL Card Installation Instructions*
8312-A2-GZ40	*Hotwire 8312/8314 ReachDSL Cards Installation Instructions*
8335-A2-GB20	*Hotwire ATM Line Cards, Models 8335, 8365, and 8385, User's Guide*
8343-A2-GZ40	*Hotwire 8343/8344 Packet SDSL Cards Installation Instructions*
8373-A2-GZ40	*Hotwire 8373/8374 RADSL Cards Installation Instructions*

Document Number	Document Title
8400-A2-GB20	*Hotwire Shelf Concentration and Processing (SCP) Card User's Guide*
8400-A2-GN20	*Hotwire Shelf Concentration and Processing (SCP) Card Installation Instructions*
8510-A2-GZ40	*Hotwire 8510 RADSL Card Installation Instructions*
8600-A2-GN20	*Hotwire 8600 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*
8610-A2-GN20	*Hotwire 8610 DSLAM Installation Guide*
8620-A2-GN20	*Hotwire 8620 GranDSLAM Installation Guide*
8700-A2-GB20	*Hotwire TDM SDSL Termination Units, Models 8777 and 8779, User's Guide*
8700-A2-GB25	*Hotwire TDM SDSL Termination Units, Models 8775 and 8785, User's Guide*
8774-A2-GB20	*Hotwire 8774 TDM SDSL Termination Unit, with DSX-1 Interface, User's Guide*
8776-A2-GB20	*Hotwire 8776 TDM SDSL Termination Unit, with G.703 Interface, User's Guide*
8784-A2-GB20	*Hotwire 8784 TDM SDSL Termination Unit, with DSX-1 Interface, User's Guide*
8786-A2-GB20	*Hotwire 8786 TDM SDSL Termination Unit, with G.703 Interface, User's Guide*
8799-A2-GB20	*Hotwire 8799 TDM SHDSL Line Card, with G.703 Interface, User's Guide*
8799-A2-GZ40	*Hotwire 8799 TDM SHDSL Line Card, with G.703 Interface, Installation Instructions*
8800-A2-GN21	*Hotwire 8800 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*
8810-A2-GN21	*Hotwire 8810 DSLAM Installation Guide*
8820-A2-GN20	*Hotwire 8820 GranDSLAM Installation Guide*

Contact your sales or service representative to order additional product documentation.

Paradyne documents are also available on the World Wide Web at **www.paradyne.com**. Select *Support* → *Technical Manuals* → *Hotwire DSL Systems*.

About the MCC Card

1

Overview

The Hotwire® Management Communications Controller (MCC) cards (MCC, MCC Plus and MCP) are processor circuit cards mounted in a Hotwire Digital Subscriber Line Access Multiplexer (DSLAM) chassis (8600, 8610, 8800, or 8810), or Hotwire GranDSLAM chassis (8620 or 8820).

Use this MCC Card . . .	In this Hotwire Chassis . . .	In this slot . . .
MCC Plus (8000-B2-111)	8600	Slot 1 of base chassis
	8800	Slot 19
	8810	Slot 19
MCP (8000-B2-211)	8610	Slot 1 of base chassis
	8620	Slot 1
	8820	Slot 9
MCP (8900-B1-211)	8620 with SCP Card	Slot 1
	8820 with SCP Card	Slot 9

MCP (Management Control Processor) and MCC Plus cards provide management for high-density port cards such as the 8312 ReachDSL 12-port card.

NOTE:

All references to MCC cards in this document refer to the MCC, MCP and MCC Plus cards, unless specifically noted otherwise.

When loaded with IP Conservative software, the MCC card provides consolidated management access for the following:

- Hotwire 8510/8373/8374 Rate Adaptive Digital Subscriber Line (RADSL) cards
- 8310 MVL® cards
- 8312/8314 ReachDSL™ version 1 (formerly MVL) cards

- 8312/8314 ReachDSL version 2 cards
- 8303/8304 Packet Integrated Services Digital Network Digital Subscriber Line (IDSL) cards
- 8343/8344 Packet Symmetric Digital Subscriber Line (SDSL) cards
- 8335/8365/8385 Asynchronous Transfer Mode (ATM) cards
- 8799 TDM Symmetric High-bit-rate Digital Subscriber Line (SHDSL) cards
- 5620 RADSL RTU Service Node
- 6310 ReachDSL v1 (formerly MVL) Modem Service Node
- 6350 ReachDSL v2 Modem Service Node
- 6301/6302 IDSL Router Service Node
- 6341/6342 SDSL Router Service Node
- 6351 ReachDSL Router Service Node
- 6371 RADSL Router Service Node

For TDM SDSL (IP Conservative) firmware release 5.0 and above, the MCC card also provides management access for Hotwire TDM SDSL Standalone Termination Units and TDM SDSL cards.

TDM SDSL and TDM SHDSL cards are not within the scope of this document.

NOTE:

All references to DSL cards refer to MVL, RADSL, ReachDSL, IDSL, SDSL, ATM, and TDM SDSL, and TDM SHDSL cards, unless specifically noted. DSL cards are also referred to as Access Nodes (ANs), and the endpoints are referred to as Service Nodes (SNs).

Features

The MCC card provides these features:

- **Diagnostics**

  Diagnose devices and network problems, perform tests in the management domain (including Ping, TraceRoute and power-on self-test).

- **Device and Test Monitoring**

  Poll device status, activate alarm indicators, log system errors, measure performance capabilities.

- **Asynchronous Terminal Interface (ATI)**

  A menu-driven VT100-compatible interface.

- **Primary Network Management Support via SNMP**

  Primary network management support through an SNMP agent for monitoring and traps.

- **Alarm Indication**

  Faceplate LEDs provide general card and Ethernet status.

- **Trap Handling**

  For all cards in chassis.

- **Non-Volatile Database Storage**

  Non-volatile database storage for configuration options and host routes.

- **Automatic Configuration Backup and Restore Functionality**

  Automatic configuration backup on a selectable schedule and user-initiated backup and restoral are available.

- **Control**

  Firmware download, configuration upload and download for all cards in the DSLAM and for Service Nodes.

- **Automatic Firmware Download**

  Allows automatic download of firmware from the MCC card's Flash File System.

- **Telnet/SNMP Access Security**

  Telnet/SNMP access based on user-specified Internet Protocol (IP) addresses.

- **RADIUS Authentication**

  RADIUS authentication of console and Telnet user logins.

Levels of Access

There are two levels of diagnostic/administrative access to the user interface via a terminal or Telnet session:

- **Administrator**

  The Administrator has complete read/write access to all cards in the chassis. With this access level you can set specific parameters and variables to configure the MCC card, its ports, its interfaces, its user accounts, and SNMP security.

- **Operator**

  The Operator has read-only access to all cards in the chassis. With this level of access you can view DSL status, physical layer status, interfaces, and IP routes, and you can run nondisruptive tests.

Access levels are configured via the Users Account screen. The default access is no login and no password with Administrator status. To provide login security to the DSL card, at least one Administrator account must be configured.

Software Functionality

MCC card software provides all the features listed above, and allows you to monitor the entire system and view pertinent status on every card in the chassis. Software functionality is provided through menu selections that are summarized below. For details on the menu hierarchy, see *Hotwire – MCC Menu* in Chapter 2, *Menus and Screens*.

The MCC Configuration Menu

The MCC Configuration Menu provides options to:

- Configure interfaces and ports
- Set up user accounts and permissions
- Authorize Telnet/SNMP access from specified sources
- Set up Radius server accounts and permissions
- Upload or download configuration
- Download new versions of software to any card in the DSLAM or to the Service Node
- Define and enable filters on the MCC interface for additional security
- Automatically backup and restore the DSLAM's configuration files
- Automatically download firmware files from the MCC card's Flash File System

NOTE:

You must have Administrator permission to configure the system. For more information about configuring the system, see Chapter 4, *Configuration Menu Options.*

The MCC Monitoring Menu

The MCC Monitoring Menu provides options to:

- View status of active ports and interfaces
- Display statistics, for example, information about an application program on a specific socket number, UDP statistics, TCP data and connection statistics, IP statistics, ICMP packet statistics, Ethernet statistics, and SNMP statistics
- Display detailed information about the MCC routing table and its entries
- Display the current Address Resolution Protocol (ARP) table
- Display information about the configured IP router filters
- Monitor FTP and TFTP transactions

The monitoring screens gather pertinent information and isolate potential problem areas. You can monitor the system with either Administrator or Operator permission. For more information, see *Chapter 5, Monitoring Menu Options.*

The MCC Applications Menu

The MCC Applications Menu provides options to:

- Perform Ping tests and display results
- Perform a TraceRoute to an IP address
- Establish a Telnet session

For more information, see Chapter 4, *Configuration Menu Options*.

The MCC Diagnostics Menu

The MCC Diagnostics Menu provides options to:

- Display self-test results for CPU, memories, and ports
- Show major and minor alarms
- Display or clear system error logs
- Enable or disable the A/B power supply alarm

For more information, see Chapter 4, *Configuration Menu Options.*

NOTE:

You must have Administrator permission to perform most diagnostic activities. For more information, see Chapter 7, *Diagnostics Menu Options*.

Menus and Screens

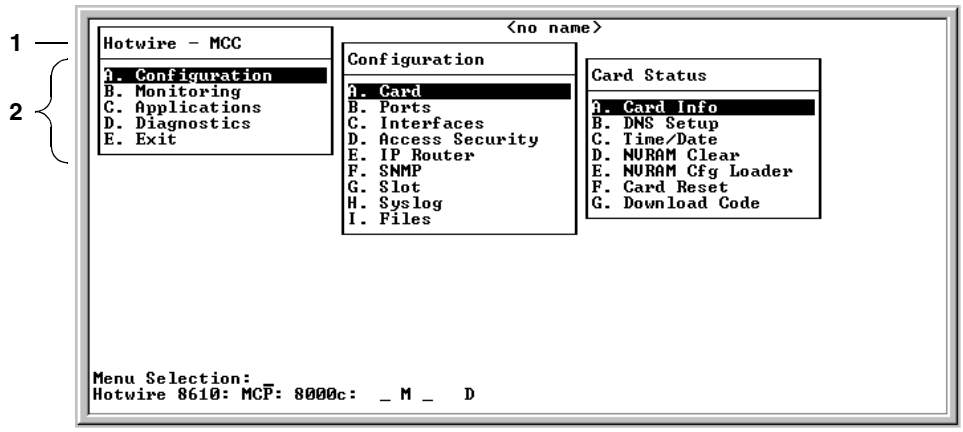
2

User Interface Formats

The Hotwire MCC user interface has ASCII text menus and screens.

Menu Components

A typical MCC menu screen looks like this:



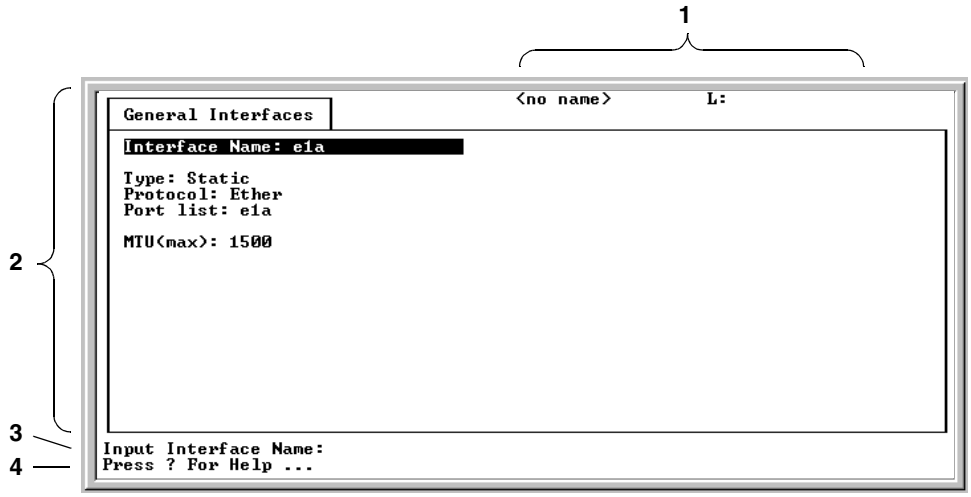
1. **Menu Title** is the top line of the boxed menu. It displays the title of the menu or submenu.
2. **Menu List** (below the menu title) displays the list of menu options. When selected, a menu option usually displays a submenu window or screen. If no submenu is shown, an input (or information) screen appears.

Alphabetical navigation keys precede each menu selection (for example, **A. Configuration**). These keys provide a convenient way to select menu items. For example, from the menu above, you press the **A** key to select the Configuration menu. The Configuration menu appears. You then press the **A** key to select the Card Status menu. The Card Status menu appears.

See *Navigation Keys* on page 2-3 for more information.

Screen Components

A typical MCC input screen looks like this:



1. **System Header Line** is the top right line of the screen. This line contains two fields of system login information:

   — The first field displays the chassis or individual card name, for example, MCC. If you have not defined the system name, **<no name>** appears.

   — The second field displays the current login.

2. **Display Area** is the main body of the screen. This area contains the screen name in a “tab” at the upper left, and fields displaying data and/or requiring input. The input values themselves are entered in the Input Line at the bottom of the screen (see Input Line description below).

3. **Input Line** is in the lower area of the screen (**Input Interface Name:** in the screen above). This area displays prompts after which you enter values for the field highlighted in the Display Area.

4. **Status Line** is the last line of the screen. It displays status about the selected card. For example,

   Hotwire 8810: MCC Plus: 8000c: __ __ __ U File Transfer in Progress

   The first field is the chassis type, in this case, the Hotwire 8810 DSLAM. The second field is the model number of the card selected, for example, the MCC Plus card model number 8000c (the c in the model number indicates IP Conservative functionality). The remaining fields indicate card information, such as whether an alarm is present. For more information about these fields, see Table 2-2, Mgmt. Card Select Screen Fields. The status line alternates each time the screen is refreshed with **Press ? For Help**.

Navigation Keys

Table 2-1. Navigation Keys

Keys	Definition
Backspace, Del, Ctrl-d	Erases the character to the left of the prompt.
Ctrl-e	Returns to the card selection screen from any screen.
Ctrl-r	Resets counters (on monitoring statistics displays).
Ctrl-u	Clears the current input or prompt line.
Ctrl-v	Displays pop-up menus.
Esc h, ?	Displays the online Help screen.
Esc l, Ctrl-l	Refreshes the screen.
Esc n	Goes to the next window.
Esc p, Ctrl-z	Goes back to the previous window.
Esc t, Ctrl-a, Ctrl-c, Ctrl-t, or Ctrl-y	Goes back to the original, top-level window.
Left arrow, Ctrl-b	Moves the cursor to the left.
Right arrow, Ctrl-f	Moves the cursor to the right.
Up arrow, Ctrl-p	Moves up to the previous menu selection or entry field.
Down arrow, Ctrl-n	Moves down or to the next selection.
Enter or Return	Accepts entry.

Accessing the System

Access the system via the User Login screen. This screen only appears if you have configured your DSL system and set up accounts on the Configure Accounts screen. If your system is new and unconfigured, go to Chapter 3, *Setup and Configuration*.

If there is no BOOTP server on the Ethernet LAN, the initial configuration must be done from the console port.

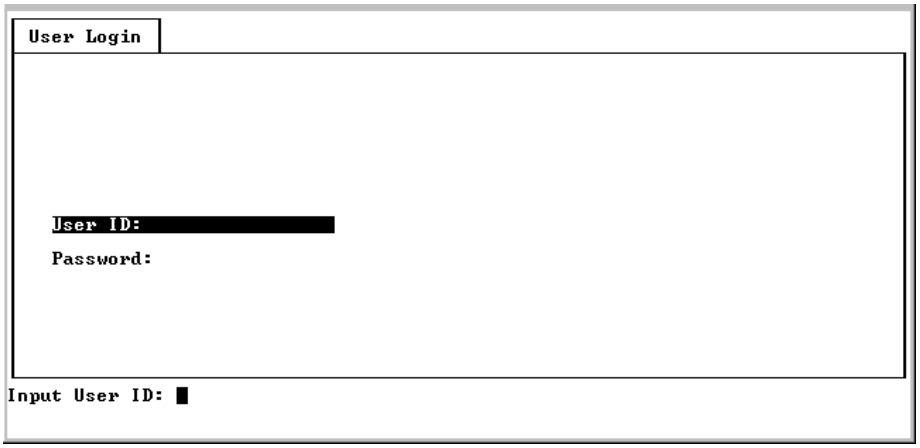
User Login Screen

You can log in to the Hotwire DSL system using either a local VT100-compatible terminal or a remote Telnet connection.

NOTE

The Hotwire DSL system accepts only one login session at a time.

At the User Login screen, enter your login ID and password.



NOTE:

The login ID and password are case-sensitive; that is, the system distinguishes between upper- and lowercase letters.

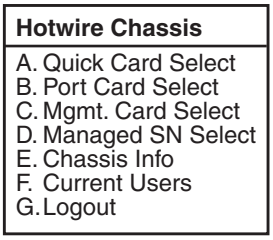
After entering your login ID and password, there may be a delay if RADIUS Authentication is in effect before the system displays the Hotwire Chassis Main Menu. This delay can be up to 12 minutes, but is usually less than one minute. The screen provides feedback of progress during the waiting period.

Hotwire Menu Structure

This section describes the menu structure of the Hotwire user interface.

Hotwire Chassis Main Menu

The Hotwire Chassis Main Menu is shown below.



From the Hotwire Chassis Main Menu, you can select:

- **A. Quick Card Select** to display a list of all cards in the chassis. Used to jump directly to an MCC or DSL card in the chassis, or to a Service Node (SN). The card you select determines the next Hotwire menu. The Quick Card Select screen also provides status on the card interfaces. After selecting a port card or SN, you can return to the Quick Card Select screen by pressing Ctrl-e.

  See *Quick Card Select Screen* on page 2-6.

- **B. Port Card Select** to select a particular port card in the chassis or display status about all port cards and their interfaces. After selecting a port card or SN, you can return to the Port Card Select screen by pressing Ctrl-e.

  See *Port Card Select Screen* on page 2-6.

- **C. Mgmt. Card Select** to select a particular management card in the chassis or display status about all management cards and their interfaces. After selecting a port card or SN, you can return to the Mgmt. Card Select screen by pressing Ctrl-e.

  See *Mgmt. Card Select Screen* on page 2-6.

- **D. Managed SN Select** to display the list of directly managed Service Nodes (SNs) and their connectivity status. After displaying the list of SNs, you can return to the Managed SN Select screen by pressing Ctrl-e.

  See *Managed SN Select Screen* on page 2-6.

- **E. Chassis Info** to enter or display chassis information, such as the chassis name, person responsible for the system, and physical location.

  See *Chassis Information Screen* on page 2-13.

- **F. Current Users** to display a list of users currently logged in Help.

  See *Current Users Screen* on page 2-13.

- **G. Logout** to exit from the current login session on the Hotwire chassis.

  See *Exiting the System* on page 2-14.

Quick Card Select Screen

This screen displays all the cards in the chassis and enables you to Telnet to a selected card in the chassis or to a connected DSL Router (for example, 6371 RADSL), providing you know the port on the DSL card to which the endpoint is connected. Select a specific card or SN and establish a connection from it to the MCC for configuring or monitoring the card. Only those slots that are populated are displayed; empty slot numbers are skipped. If more than 17 slots are populated, 15 cards will display on a first page, with the remaining slots displaying on a second page.

NOTE:

If a card is locked in Download Only mode, you will be informed of this and no status will display on the screen.

Port Card Select Screen

This screen displays all DSL port cards in the chassis and enables you to Telnet to a selected DSL card in the chassis or to a connected DSL Router (for example, 6371 RADSL), providing you know the port on the DSL card to which the endpoint is connected. Only those slots that are populated are displayed; empty slot numbers are skipped. Only six or seven DSL cards can fit onto one page, so multiple pages may be required to display status for all DSL port cards in the chassis.

NOTE:

If a card is locked in Download Only mode, you will be informed of this and no status will display on the screen.

Mgmt. Card Select Screen

This screen displays all MCC-type management cards in the chassis and enables you to Telnet to a selected MCC card in the chassis or to a connected DSL Router (for example, 6371 RADSL), providing you know the port on the DSL card to which the endpoint is connected. For Hotwire GranDSLAM chassis, SCM cards are also listed on this screen.

NOTE:

If a card is locked in Download Only mode, you will be informed of this and no status will display on the screen.

Managed SN Select Screen

This screen displays all SNs connected to DSL port cards in the chassis. It also enables you to Telnet to a selected SN with advanced services by entering the slot and port number of the AN (port card) to which desired SN connected.

Accessing a Selection Screen

▶ Procedure

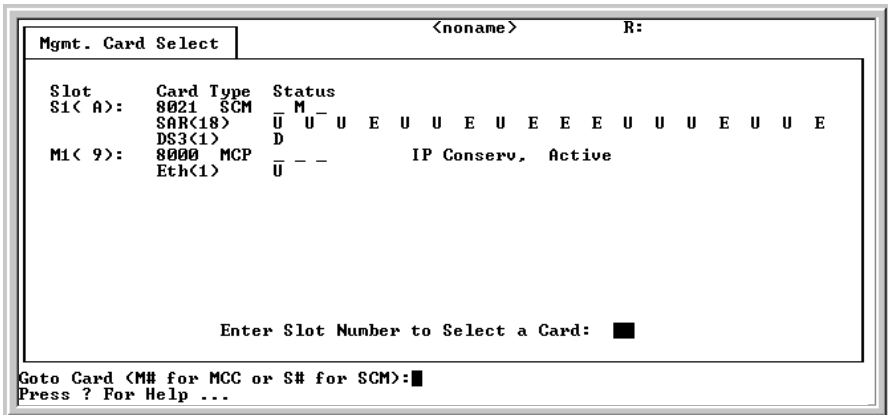
To access one of the card selection screens:

1. From the Hotwire Chassis Main Menu, select one of the following:
   - — **A** for Quick Card Select
   - — **B** for Port Card Select
   - — **C** for Mgmt. Card Select
   - — **D** for Managed SN Select

   The desired selection screen appears.
2. At the **`Goto:`** prompt, type the slot number of the desired card. Or, type the slot and port number of the desired SN.

   The appropriate menu appears. For port card menu information, see the *Hotwire MVL, ReachDSL, RADSL, IDSL, and SDSL Cards, Models 8310, 8312/8314, 8510/8373/8374, 8303/8304, and 8343/8344, User's Guide*, the *Hotwire ATM Line Cards, Models 8335, 8365, and 8385, User's Guide*, or the appropriate TDM SDSL or TDM SHDSL User's Guide. For SN menu information, see the *Hotwire DSL Routers User's Guide*. For SCM card menu information, see the *Hotwire Shelf Concentration Module (SCM) Card User's Guide*.

   See the following for an example Mgmt. Card Select screen.


<noname> R:
Mgmt. Card Select
Slot Card Type Status
S1(A): 8021 SCM _ M _
SAR(18) U U U E U U E U E E E U U U E U U E
DS3(1) D
M1(9): 8000 MCP _ _ _ IP Conserv. Active
Eth(1) U
Enter Slot Number to Select a Card:
Goto Card (M# for MCC or S# for SCM):
Press ? For Help ...

NOTE:

If an option is not active, an underscore appears in its place.

The information in Table 2-2, Mgmt. Card Select Screen Fields, is displayed on the Mgmt. Card Select screen.

Table 2-2. Mgmt. Card Select Screen Fields

Column Heading	Display		Description
Slot	M1<slot number>		Management card
Card Type	<card type>		Management card model number (8000) and card type: MCC, MCC+, MCP
Status 1st line	Position 1: T or _		Test mode. Card currently in test mode or _ for no active test.
	Position 2: M or _		Major alarm. Major alarm present on card or _ for no active major alarm.
	Position 3: R or _		Minor alarm. Minor alarm present on card or _ for no minor alarm active.
	<descriptive text>		Up to 42 characters of additional information about the card (IP Conservative software) and status of the card (Active or Spare)
Status 2nd line	<status>	U, D, X, L, or A	Uplink type (for example, Eth) and status of uplink: U=Up, D=Down, X=Disabled, L=Loopback (uplink only), A=Alarm (uplink only), E=Empty slot

For example, the following may be displayed on the Mgmt. Card Select screen:

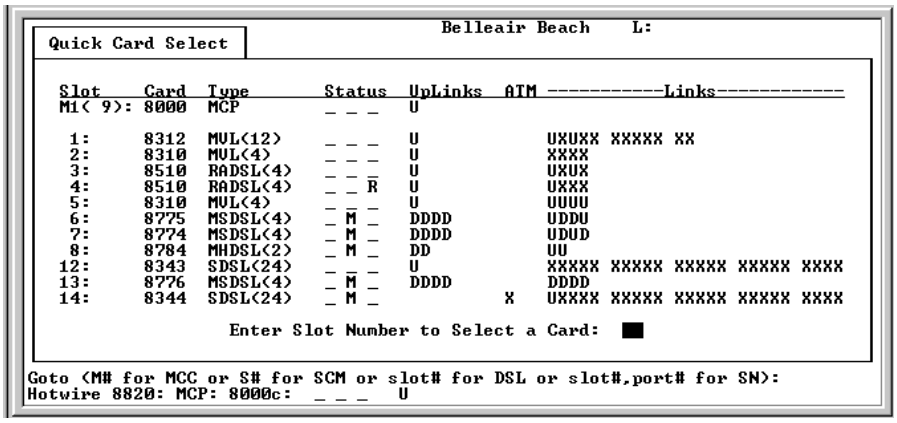
```
Line 1:   M1(1)  8000  MCP   _ _ _     IP Conserv, Active
Line 2:          Eth(1)      U

Position:                     1 2 3
```

Line 1 shows the following:

- There is an MCP card in Slot 1
- Position 1 – No current test (_)
- Position 2 – No major alarm is present (_)
- Position 3 – No minor alarm present (_)
- IP Conservative software is running and the MCP card is active

Line 2 shows that there is an Ethernet uplink and the link is up.

The following is an example of the Quick Card Select screen.


Belleair Beach L:
Quick Card Select
Slot Card Type Status UpLinks ATM ----------Links----------
M1(9): 8000 MCP _ _ _ U
1: 8312 MVL(12) _ _ _ U UXUXX XXXXX XX
2: 8310 MVL(4) _ _ _ U XXXX
3: 8510 RADSL(4) _ _ _ U UXUX
4: 8510 RADSL(4) _ _ R U UXXX
5: 8310 MVL(4) _ _ _ U UUUU
6: 8775 MSDSL(4) _ M _ DDDD UDDU
7: 8774 MSDSL(4) _ M _ DDDD UDUD
8: 8784 MHDSL(2) _ M _ DD UU
12: 8343 SDSL(24) _ _ _ U XXXXX XXXXX XXXXX XXXXX XXXX
13: 8776 MSDSL(4) _ M _ DDDD DDDD
14: 8344 SDSL(24) _ M _ X UXXXX XXXXX XXXXX XXXXX XXXX
Enter Slot Number to Select a Card:
Goto (M# for MCC or S# for SCM or slot# for DSL or slot#,port# for SN):
Hotwire 8820: MCP: 8000c: _ _ _ U

NOTES:

— If an option is not active, an underscore appears in its place.

— The 8312/8314 ReachDSL v1 cards appear on the screen with their former MVL name.

The information in Table 2-3, Quick Card Select Screen Fields, is displayed on the Quick Card Select screen.

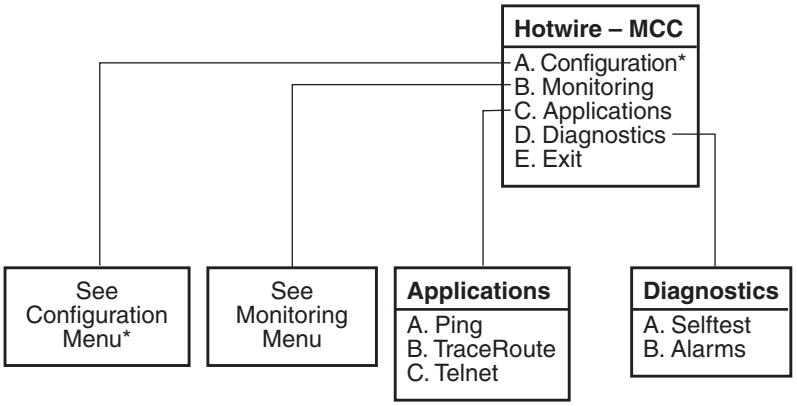
Table 2-3. Quick Card Select Screen Fields

Column Heading	Display	Description
Slot	<slot number>	Slot number of card in chassis.
Card	<model number>	Model number of card, such as 8312, 8343, etc.
Type	RADSL, SDSL, etc. (1–24)	Card type (number of ports), for example SDSL(24).
Status	Position 1: T or _	Test mode. Card currently in test mode or _ for no active test.
	Position 2: M or _	Major alarm. Major alarm present on card or _ for no active major alarm.
	Position 3: R or _	Minor alarm. Minor alarm present on card or _ for no minor alarm active.
UpLinks	<uplink status>	Status of uplink: U=Up, D=Down, X=Disabled/Not Initialized, L=Loopback, A=Alarm
ATM	<atm status>	Status of ATM uplink: U=Up, D=Down
Links	<dsllink status>	Status of DSL ports: U=Up, D=Down, X=Disabled/Not Initialized, L=Loopback, E=Empty slot, I=Incompatible slot, H=Handshaking, N=Network timing

Hotwire – MCC Menu

After selecting the MCC card from either the Quick Card Select screen or the Mgmt. Card Select screen, the system displays the Hotwire – MCC Menu.

From this menu you configure, monitor, run applications, and diagnose the MCC card.



* The Configuration menu item appears only if you have Administrator permission.

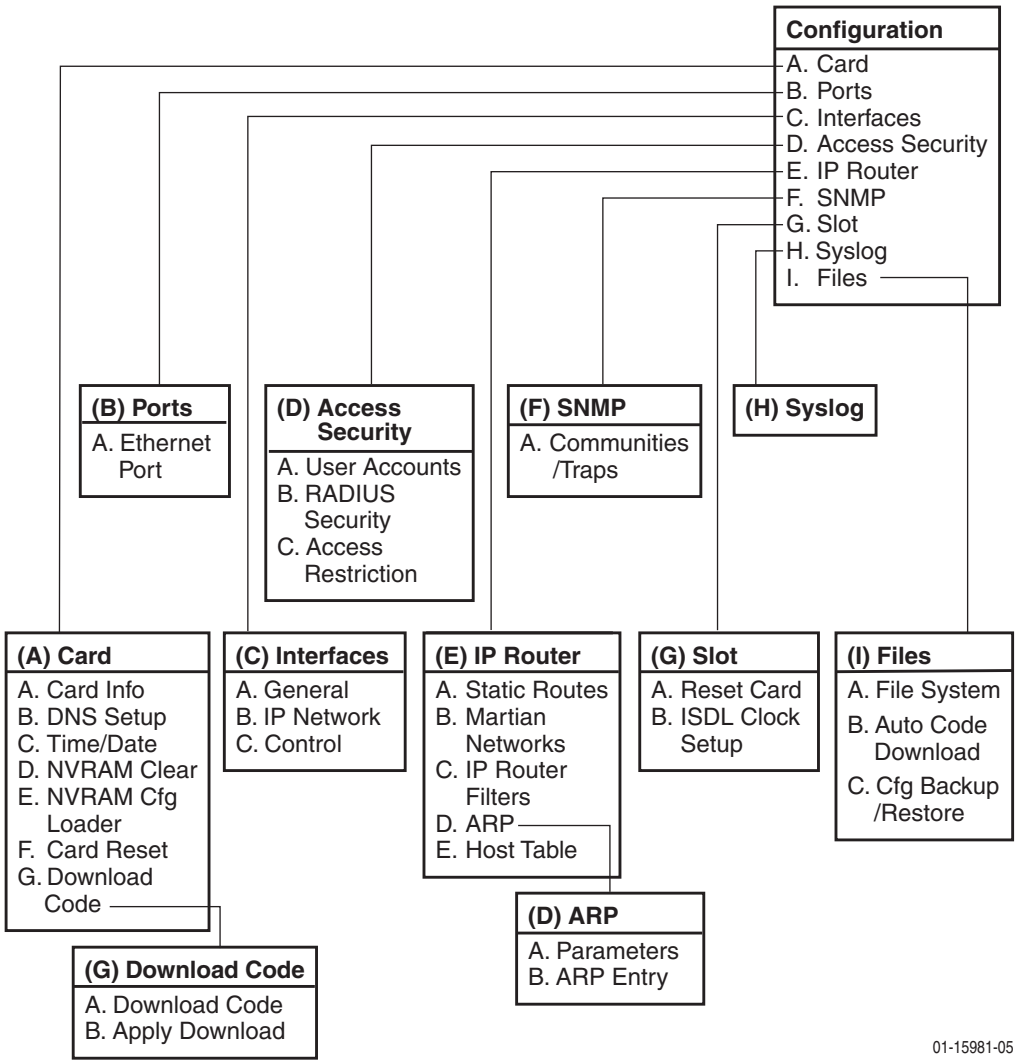
01-15980-01

Configuration Menu

The following figure illustrates the complete Configuration menu hierarchy selected from the Hotwire – MCC menu.

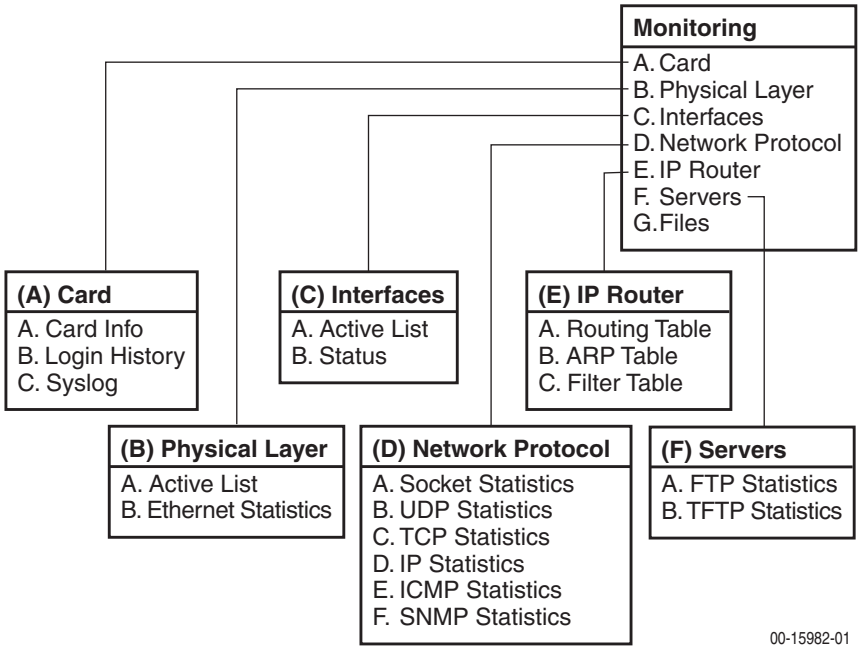
NOTE:

The Configuration Menu selection only appears if you log in to the system with a user account that has Administrator permission.



Monitoring Menu

The following figure illustrates the complete Monitoring Menu hierarchy selected from the Hotwire – MCC Menu.



Applications Menu

The Applications menu contains three selections:

- **A.** Ping
- **B.** TraceRoute
- **C.** Telnet

Diagnostics Menu

The Diagnostics menu contains two selections:

- **A.** Selftest
- **B.** Alarms

Chassis Information Screen

Table 2-4. Chassis Information Screen Fields

Field	Input Characters	Description
Chassis Name	16 alphanumeric	Name for the equipment.
Chassis Contact	32 alphanumeric	Name and phone number of individual responsible for the equipment.
Chassis Location	16 alphanumeric	Physical location of the equipment.
Bay Number	16 alphanumeric	Floor and/or bay number of the equipment.
Chassis Number	16 alphanumeric	Chassis serial number (located on the lower right side of chassis).
Chassis Model	4 alphanumeric	Chassis model number (8600, 8800, 8610, 8810, or Hotwire 8620 or 8820 GranDSLAM). The MCC card fills in this field, but you can change it. You must reset the MCC for your change to take effect.
Serial Number	8 alphanumeric	Chassis serial number (Model 8620 only).
SIM	2 alphanumeric	System Interface Module (SIM) type (Model 8620 only).
Serial Num	8 alphanumeric	SIM serial number (Model 8620 only).
Hardware Rev	8 alphanumeric	Hardware revision number (Model 8620 only).

Use care when filling in this information, since the system will react based on the values you enter. Filling in this information results in adding data in the MIB II Systems Group.

After you have made changes, the message **`Configuration has been modified. Save (yes/no)?`** appears. Type **`y`** or **`yes`** and press Enter to save changes. The Hotwire Chassis Main Menu appears.

Current Users Screen

Table 2-5. Current Users Screen Fields

Field	Description
User ID	User ID of the person logged in.
Time	Login time.
Priv	Access level assigned to the user who logged in.
Console/Telnet/FTP	The type of login (C, T, or F). If Telnet (T) or FTP (F), the IP address of the remote host is also recorded.

Exiting the System

You can manually log out of the system or, after five minutes of inactivity, the system automatically logs you out.

Manually Logging Out

▶ Procedure

To exit from the Hotwire DSL system:

1. Select Exit from either the Hotwire – MCC menu or the Hotwire – DSL menu.

   The card selection screen appears.

2. Press Ctrl-a.

   The Hotwire Chassis Main Menu appears.

3. Select **C**. Logout.

   The system exits from the current session.

Automatically Logging Off

The DSL system has an automatic timeout feature that logs you out after five minutes of inactivity. You need to log back in to continue your work.

To log back in, press Enter to display the User Login screen and log in.

Setup and Configuration

3

Overview

This chapter explains how to access the system for the first time and perform initial setup operations. It also summarizes the minimum MCC card configuration tasks. To customize your application or to obtain detailed instructions for other configuration tasks, see Chapter 4, *Configuration Menu Options*.

Interface Naming Convention

- **Eth1** is used throughout this guide to reference the 10BaseT Ethernet interface on the MCC card.
- **Ports** refers to the physical layer attributes of an interface.
- **Interface** refers to the higher level protocol running over the physical layer.

Domain Types

To monitor and control the overall system, the Hotwire Access Network should be partitioned into two distinct domains:

- Service domain(s) (Layer 2, MAC Bridging)
- Management domain (Layer 3, IP Routing)

It is recommended that the management domain reside in a separate domain from the service domain through the IPC for security purposes and to improve download performance.

Service Domain

A service (or data) domain is comprised of all clients and servers (grouped physically or virtually) that communicate across a common WAN or LAN connection for Internet or intranet access. This is the Layer 2 bridging domain of the NSP. The Access Node cards and the Service Nodes are the Hotwire components of this domain. The service domain also encompasses an NSP and all end-user systems that subscribe to that NSP.

NOTE:

TDM SDSL products are not packet devices and are not part of the Service domain.

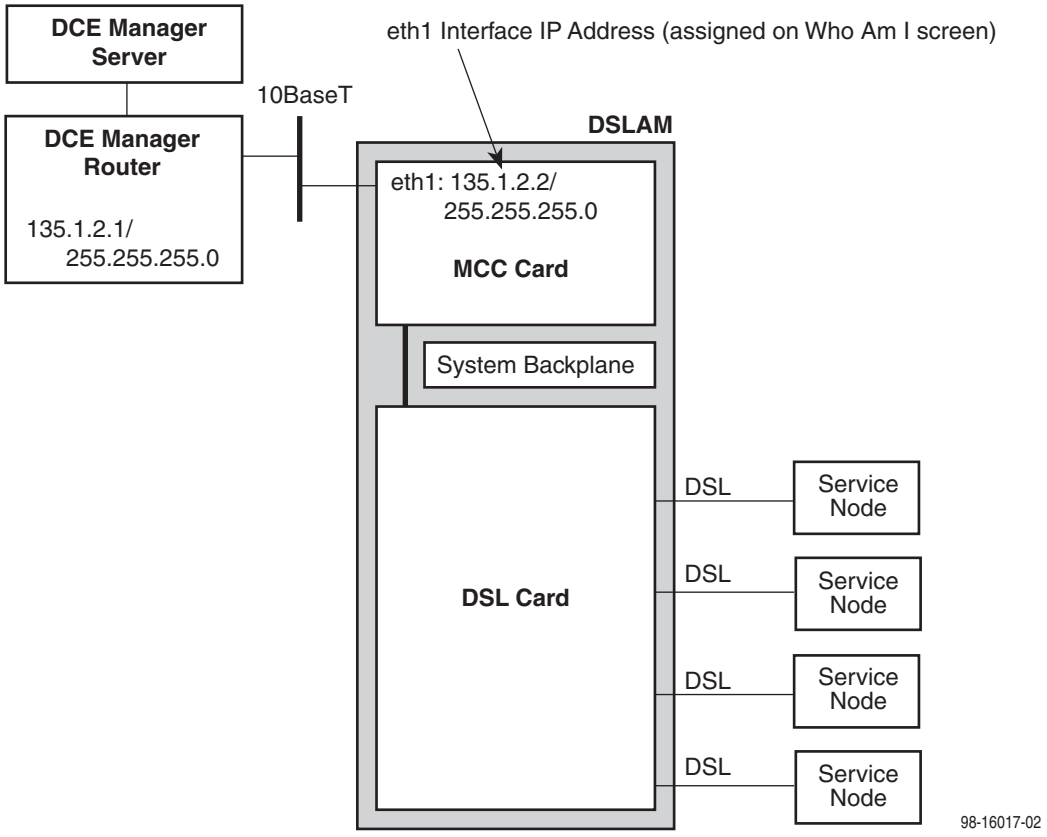
Management Domain

The primary function of the Management domain is monitoring and configuring the DSL cards and service domains served by the cards. The management domain should reside in a mutually exclusive domain from that of the service (data) domain(s). The MCC card functions as a service router and is the primary tool for configuring and diagnosing the management domain.

To configure the management domain, see *Management Domain Configuration* on page 3-6.

Management Domain Components

The following illustrates management domain components that *must* be configured, and gives examples of the various naming conventions.



Accessing the System for the First Time

After powering the system on for the first time, you must set the management IP address and subnet mask of the MCC card. This is a mandatory step and *must* be completed before proceeding. Either enter this address at the local console, or have the MCC receive the information via BOOTP over the Eth1 Ethernet interface.

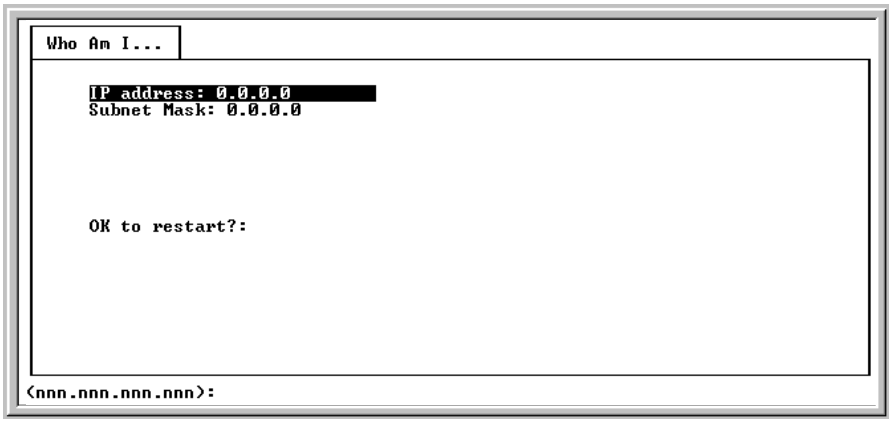
To ease configuration and reduce the number of IP addresses needed by the DSL system, only the MCC card is assigned a globally available, public IP address. All of the Access Node (AN) port cards, as well as the TDM SDSL cards, have IP addresses for management, but they are special internal addresses and are not reported to the network. The MCC is the address translator for all management traffic to and from the DSL cards.

▶ Procedure

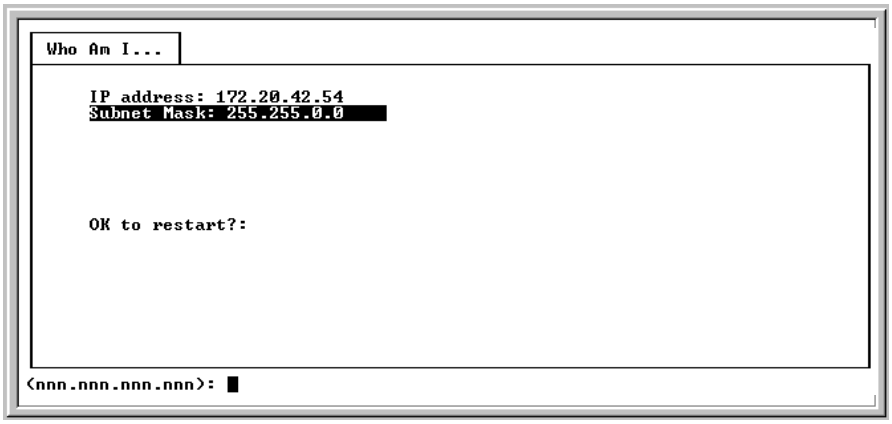
To set the MCC's management IP address and subnet mask from the console terminal:

1. Power up the chassis.

   After the self-test completes, the Who Am I screen appears.



2. From the Who Am I screen, enter the management domain IP address of the MCC card and press the Enter key. For example, if the IP address of the MCC card is **198.152.110.1**, type this value at the **`(nnn.nnn.nnn.nnn):`** prompt on the Input Line at the bottom of the screen.



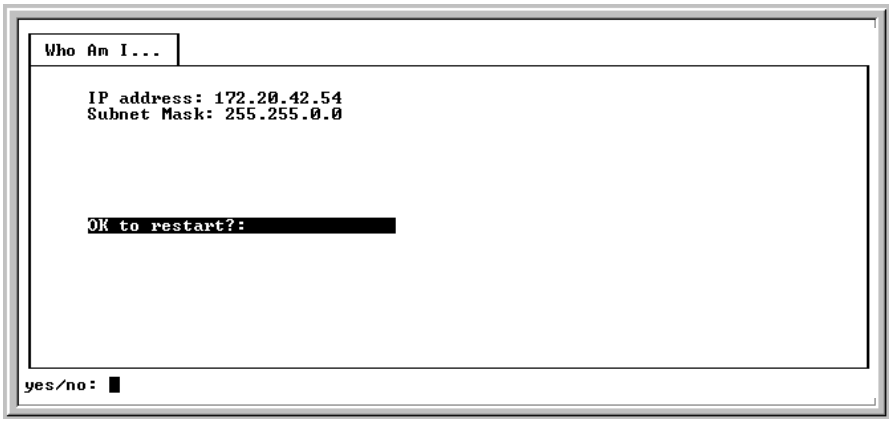
The system automatically calculates the subnet mask based on the IP address you enter.

3. Do one of the following at the **(nnn.nnn.nnn.nnn):** prompt:

   — To accept the subnet mask, press Enter.

   — To change the subnet mask, enter a new subnet mask and press Enter.

   The system highlights the **OK to restart?:** prompt.



4. Type **y** at the **yes/no:** prompt to restart the card (or **n** to decline the restart).

   If you type **y**, the card restarts. The Hotwire Chassis Main Menu appears.

   While this screen is present, the MCC is sending BOOTP requests over the Ethernet interface. Should a BOOTP response be received before manual configuration is complete, the IP address and subnet mask assigned by the BOOTP server will be used and the card will automatically reset.

   NOTE:

   The MCC card can now accept a Telnet session for remote configuration, but it is recommended that you first define user accounts to provide security to the DSL cards.

Management Domain Configuration

The following table lists the basic steps you need to configure the MCC card after you have assigned an IP address.

On the MCC Card in the Management Domain, to . . .	See . . .
1. Create the Default Route	*Task 1: Creating the Default Route*.
2. Create community strings and enable RADIUS Authentication	*Task 2: Creating SNMP Community Strings and Enabling Authentication Failure Traps* on page 3-7.

NOTE:

It is assumed that you have read the *Hotwire MVL, ReachDSL, RADSL, IDSL, and SDSL Cards, Models 8310, 8312/8314, 8510/8373/8374, 8303/8304, and 8343/8344, User's Guide*, the *Hotwire ATM Line Cards, Models 8335, 8365, and 8385, User's Guide*, or the appropriate TDM SDSL or TDM SHDSL User's Guide. See *Product-Related Documents* in *About This Guide*.

Task 1: Creating the Default Route

This procedure creates the default route to the management domain next hop router. This default route forwards management domain traffic from the MCC card.

▶ Procedure

To create the default route for management domain traffic *from* the MCC card:

1. Select *Configuration*→*IP Router*→*Static Routes* (**A-E-A**).
2. Type **0** (zero) or press Enter at the **`Item Number`** prompt.
3. Type **0.0.0.0** at the **`Destination (or space to delete route):`** prompt for Host/Net and press Enter. You can also type the word **default**.
4. Press Enter at the **`Subnet Mask:(nnn.nnn.nnn.nnn)`** prompt.
5. Type the IP address of the default route to the next hop address at the **`Next Hop IP Address (nnn.nnn.nnn.nnn)`** prompt and press Enter.
6. Type **1** for preference at the **`Input Number`** prompt and press Enter.
7. Leave default fields for **`S/D`** (Source/Destination) and **`PA`** (Proxy ARP) fields.
8. Type **y** to save the changes.

Task 2: Creating SNMP Community Strings and Enabling Authentication Failure Traps

Use this procedure to configure SNMP community strings and enable the Authentication Failure trap mechanism for all cards. These procedures provide a minimal level of security. For additional security, ensure that Source validation and/or Radius validation is enabled.

▶ Procedure

1. From the MCC Main Menu, select *Configuration→ SNMP →* *Communities/Traps (***A-F-A**).

   The SNMP Communities/Traps screen appears. The Authentication Failure Trap: field is highlighted. Your response at the prompt determines whether the Authentication Failure Trap mechanism is enabled or disabled on the MCC card.

2. Type your desired response at the **`Enable/Disable:`** prompt and press Enter.

   The first community string name field is highlighted (default name: public). This community string has read-only permission.

3. Press Enter to accept the default name, or type the community string name(s) you wish to enter at the **`Community Name:`** prompt and press Enter.

   The permissions field is highlighted.

4. Press Enter to accept the default (read-only) permission for this community string or change the permission at the prompt and press Enter.

   The IP address field is highlighted. This is the IP address of the NMS manager to which SNMP traps are sent.

5. For trap destination, type the IP address of the NMS manager at the **`IP Address nnn.nnn.nnn.nnn (or space to delete):`** prompt and press Enter. You can enter up to 12 addresses.

   The Port Input Number field is highlighted.

6. Enter the port number at the **`Input Number:`** prompt and press Enter. The default of 162 is generally used.

   The Enable/Disable field is highlighted. This field determines whether *any* trap messages are sent to the specified destination for each address.

7. Type your response at the **`Enable/Disable:`** prompt and press Enter.

   The second IP Address field is highlighted. Repeat the procedures as needed to define other NMS managers.

8. Press Ctrl-z. The **`Configuration has been modified. Save (yes/no):`** prompt appears. Enter your desired response.

You can repeat the procedures and create different levels of security for other IP addresses within the same community string and for other community strings.

Configuration Menu Options

4

Overview

This chapter describes the options on the Configuration Menu of the MCC card. Use these options to configure your MCC card and customize DSL system applications.

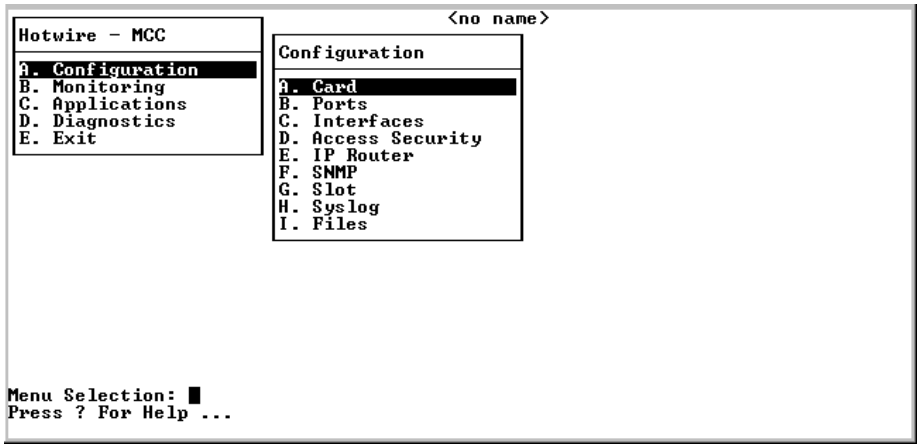
NOTE:

You must have Administrator permission to configure the MCC card.

To access the Configuration menu, follow this menu selection sequence:

MCC Menu → Configuration

The Configuration menu appears.



Configuration Menu Overview

Table 4-1, Configuration Menu Options, summarizes the options available when you select Configuration on the Hotwire MCC – Main Menu. Options are arranged into functional groups.

Table 4-1. Configuration Menu Options (1 of 2)

Select . . .	To Access the . . .	To . . .
A. Card	Card Status Menu Options (Table 4-2)	■ Configure MCC card information ■ Set up DNS servers ■ Configure local time/date ■ Clear NVRAM ■ Upload and download configurations (NVRAM Cfg Loader) ■ Reset the MCC card ■ Download new firmware
B. Ports	Ports Menu Options (Table 4-3)	■ Configure e1a as full or half-duplex ■ Reset the ports
C. Interfaces	Interfaces Menu Options (Table 4-4)	■ Configure the MTU ■ Configure up to 16 addresses for the e1a port ■ Control the state of the interface
D. Access Security	Access Security Menu Options (Table 4-5)	■ Add, delete or edit a user from a system account, and edit user passwords and privileges ■ Enable RADIUS Authentication for user logins ■ Enable/disable Telnet/SNMP access to the MCC's Ethernet port ■ Enable/Disable source address verification
E. IP Router	IP Router Menu Options (Table 4-6)	■ Add/delete static routes ■ Build list of invalid addresses ■ Set up the IP router filters ■ Build name sets of filter rules ■ Configure and add entries to the ARP cache ■ Define mappings between IP addresses and host names
F. SNMP	SNMP Menu Options (Table 4-7)	■ Set up SNMP communities/traps
G. Slot	Slot (DSL Cards) Menu Options (Table 4-8)	■ Reset a card ■ IDSL Clock Setup
H. Syslog	SYSLOG Option (Table 4-9)	■ Customize information recorded in the SYSLOG ■ Customize SYSLOG messages

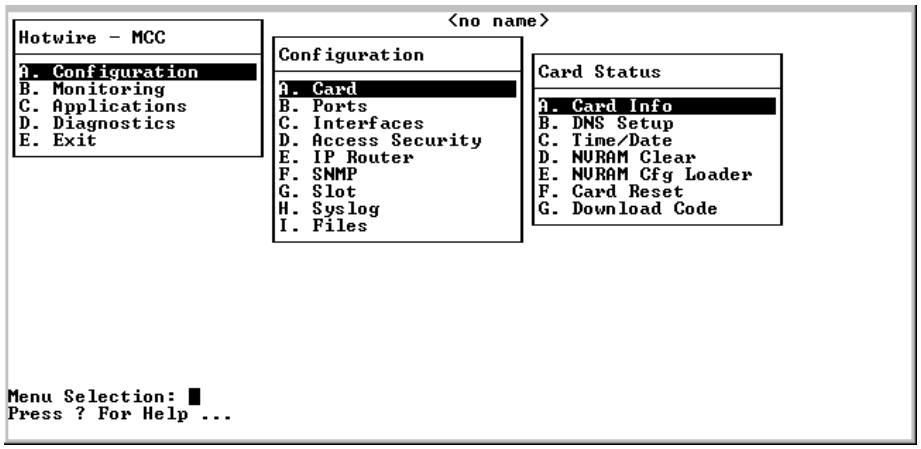
Table 4-1. Configuration Menu Options (2 of 2)

Select . . .	To Access the . . .	To . . .
I. Files	Files Menu Options (Table 4-10)	■ Change working directories ■ List subdirectories ■ Automatically download firmware files stored in the MCP's Flash File System to cards in the DSLAM ■ Schedule automatic backup of card configuration ■ Back up/restore configuration files

Card Status Menu

To access the Card Status menu, follow this menu selection sequence:

Configuration→ *Card* (**A-A**)



The Card Status menu provides the following selections:

- **A. Card Info** – Sets up MCC card information.
- **B. DNS Setup** – Sets up Domain Name System (DNS) servers.
- **C. Time/Date** – Configures local time and date.
- **D. NVRAM Clear** – Clears non-volatile RAM.
- **E. NVRAM Cfg Loader** – Uploads and downloads configurations.
- **F. Card Reset** – Resets MCC card in the chassis.
- **G. Download Code** – Downloads and applies new firmware to the MCC in an Access Node or Service Node.

See Table 4-2, Card Status Menu Options, for information about the options available from the Card Status menu.

Entering Card Information

Use the Card Information screen to configure basic card-level information. Fields on this screen are null until you enter values. Allowable values are:

- Numeric characters (0–9)
- Upper- or lowercase alphabetic characters (A–Z)
- Space
- Special characters available on standard keyboards (!, @, #, $, etc.)

▶ Procedure

To enter card-level information:

1. Follow this menu selection sequence:

   Configuration→ *Card* → *Card Info* (**A-A-A**)

   The Card Information screen appears.

2. Type the desired value in each field and press Enter. Use the left and right arrow keys to scroll through the fields. See Table 4-2, Card Status Menu Options.

3. Press Ctrl-z to save the changes and return to the Card menu.

Configuring Access to DNS Servers

Use the Configure Domain Name Server (DNS) screen to set up access to DNS servers from which host name to IP address translation requests are made. If you have configured a DNS server, then you can use the host name in lieu of its IP address in the remaining configuration.

▶ Procedure

To configure DNS servers:

1. Follow this menu selection sequence:

   Configuration→ *Card* → *DNS Setup* (**A-A-B**)

   The Configure DNS screen appears.

2. Type the desired value in each field and press Enter. See Table 4-2, Card Status Menu Options.

3. Press Ctrl-z to save the changes and return to the Card menu.

Setting the Time and Date

Use the Time/Date screen to configure the local time and date on the MCC card. The MCC's clock can be synchronized with network time through a Network Time Protocol (NTP) server.

▶ Procedure

To set the local time and date, and to configure the NTP server:

1. Follow this menu selection sequence:

   Configuration→*Card*→*Time/Date* (**A-A-C**)

   The Time/Date screen appears.

2. Type the desired value in each field and press Enter. See Table 4-2, Card Status Menu Options.

3. Press Ctrl-z to save the changes and return to the Card Status menu.

Clearing NVRAM

The NVRAM Clear screen clears Non-Volatile RAM (NVRAM). You may want to clear the NVRAM to reuse the MCC card or to reconfigure the current card. It is recommended that NVRAM be cleared after a new major firmware release has been downloaded.

Save your configuration using the NVRAM Cfg Loader (**A-A-E**) screen before clearing NVRAM.

CAUTION:

If you select yes on the NVRAM Clear screen, you permanently remove the configuration information stored on the card. All IP addresses and routing tables will need to be reentered. The system performs a reset and returns to the factory configuration.

▶ Procedure

To clear NVRAM:

1. Follow this menu selection sequence:

   Configuration→ *Card*→*NVRAM Clear* (**A-A-D**)

   The NVRAM Clear screen appears. See Table 4-2, Card Status Menu Options.

2. At the **`Initialize NVRAM:`** prompt, do one of the following:

   — Type **yes** to clear the NVRAM and return to default values.

   — Type **no** to perform no action.

   The system beeps and no action is taken.

3. Press Ctrl-z to return to the Card menu.

Uploading/Downloading Configuration Data from a TFTP Server (NVRAM Config Loader)

Use the NVRAM Config Loader screen to upload configurations to and download the MCC's configuration from a Trivial File Transfer Protocol (TFTP) server.

▶ Procedure

To upload or download NVRAM configuration data:

1. Follow this menu selection sequence:

   Configuration→ *Card*→ *NVRAM Cfg Loader* (**A-A-E**)

   The NVRAM Cfg Loader screen appears.

2. Type the desired value in each field and press Enter. See Table 4-2, Card Status Menu Options.

   When the transfer completes, the Transfer Status field changes to **`Completed successfully`** and the screen displays the following information:

   `Packets Sent` – Number of packets sent in download.

   `Packets Received` – Number of packets received in download.

   `Bytes Sent` – Number of bytes sent in download.

   `Bytes Received` – Number of bytes received in download.

   `Transfer Time` – The length of time the transfer is taking.

   `Status` – The progress of the transfer.

3. Press Ctrl-z to return to the Card menu.

   NOTE:

   After a download, the MCC card must be reset for the new configuration to take effect.

Resetting the MCC Card

Use the Card Reset screen to reset the MCC card. This command resets all counters to zero. If a new configuration or software version has been downloaded, a card reset allows the new code to become active.

NOTE:

An MCC card reset does not interrupt user data traffic on other cards in the chassis.

▶ Procedure

To reset the MCC card:

1. Follow this menu selection sequence:

   Configuration→ *Card*→ *Card Reset* (**A-A-F**)

   The Card Reset screen appears. The top of the screen says **`Other users are currently accessing the chassis, continue? no`**

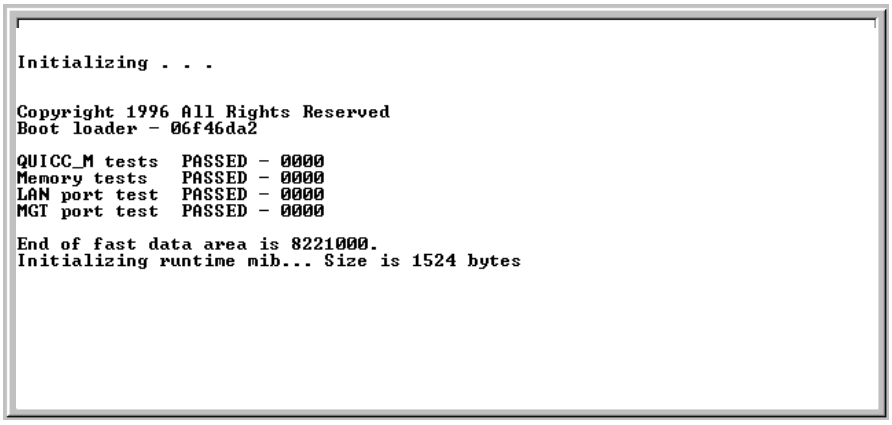
2. At the **`Reset Card:`** prompt, do one of the following:

   — Type **yes** to reset the card.

   All counters will be reset, and if a new version of software has been downloaded, then the new code will become active. This action disrupts operation of the MCC card for at least 10 seconds.

   NOTE:

   An MCC card reset logs you out of the Hotwire DSL system. You must reenter to continue.


Initializing . . .
Copyright 1996 All Rights Reserved
Boot loader - 06f46da2
QUICC_M tests PASSED - 0000
Memory tests PASSED - 0000
LAN port test PASSED - 0000
MGT port test PASSED - 0000
End of fast data area is 8221000.
Initializing runtime mib... Size is 1524 bytes

   — Type **no** to perform no action.

   The system beeps and no action is taken.

   — Press Ctrl-z to return to the Card menu without resetting the card.

Downloading Code

The Download Code menu option gives you the ability to upgrade your software with a new version of code and then apply this code to your system. See Appendix A, *Upgrade Procedures*, for additional information. See the appropriate document for TDM SDSL or TDM SHDSL download information in *Product-Related Documents* in *About This Guide*.

New firmware releases are typically applied to the MCC or DSL cards, or to the Service Node in your system. When a software upgrade affects both the MCC and the DSL cards, you must download and apply a new version of code to the DSL cards **before** you download and apply a new version of code into the MCC.

When you are downloading code to an endpoint, verify that your TFTP server has the following timeout values, or your download may fail:

- **Retransmission timeout** – Value not less than 10 seconds.
- **Total transmission** – Value not less than three times the retransmission timeout.

NOTE:

Before initiating a download, verify that you can ping the TFTP server from the MCC card. If you cannot, do not proceed with the download. Also, make certain that the files you are going to download exist on the server.

Card Status Menu Options

For Card Status menu options, refer to Table 4-2, Card Status Menu Options. To access the Card Status menu, follow this menu selection sequence:

MCC Main Menu→ *Configuration*→ *Card* (**A-A**)

Table 4-2. Card Status Menu Options (1 of 4)

Card Info	**A-A-A**
Gives you the ability to configure basic card-level information. **Card Name** – Up to 16 alphanumeric characters. Name assigned to the card. **Card Contact** – Up to 32 alphanumeric characters. Name or number of party responsible for card. **Card Location** – Up to16 alphanumeric characters. Location assigned to the system. **Router ID** – (Read-only) Displays the Management Domain IP address assigned to card in *nnn.nnn.nnn.nnn* format. **Router Subnet Mask** – (Read-only) Displays the subnet mask of the router in *nnn.nnn.nnn.nnn* format. **Local Control Terminal Port Mode** – The terminal port mode for the local or console session: Standard or Extended (Default = Standard). Standard is for USA keyboards; Extended is for European keyboards. **Remote Control Terminal Port Mode** – The terminal port mode for the Telnet session: Standard or Extended (Default = Standard). Standard is for USA keyboards; Extended is for European keyboards. **Telnet daemon tcp port** – The TCP port number that the Telnet daemon listens on. 0–59999 (Default = 23). If you change this field, you need to do a card reset. If you change this value, you must also make the same change on every Access Node. **FTP daemon tcp port** – The TCP port number that the FTP daemon listens on. 0–59999 (Default = 21). **FTP daemon tcp port (Data)** – The TCP port number that the FTP data is on. 0–59999 (Default = 20). **Alarm on loss of Redundant Power** – Enter **Y** if carrier has redundant power and you want local and remote indications of the loss of one power source. Enter **N** if there is only one power source.	
DNS Setup	**A-A-B**
Gives you the ability to configure access to DNS servers from which name-to-IP-address translation requests are made. **DNS Servers** – Three entry fields in *nnn.nnn.nnn.nnn* format. Enter the primary Domain Name System Server address. **Default Domain Name** – Up to 40 characters. Domain for queries that are not fully qualified. For example, if the default domain name = paradyne.com and a Telnet is attempted to a system called gemini, the card would query the DNS server for gemini.paradyne.com. **Time to wait for response** (**secs**) – 1–300 seconds (Default = 5). Enter the time to wait for a response. **Number of times to retry server** – 1–10 times (Default = 2). Enter the number of times to retry the server.	

Table 4-2. Card Status Menu Options (2 of 4)

Time/Date		**A-A-C**
Gives you the ability to configure the local time and date on the DSL card with network time and to synchronize DSL system clock via a Network Time Protocol (NTP) server.		
Timezone – Time zone location:		
Australia/North	Canada/Pacific	Libya
Australia/NSW	Canada/Yukon	Mexico/BajaNorte
Australia/Queensland	Chile/Continental	Mexico/BajaSur
Australia/South	Chile/EasterIsland	Mexico/General
Australia/Tasmania	China/HongKong	NewZealand
Australia/Victoria	China/PRC	Singapore
Australia/West	China/ROC	Turkey
Australia/Yancowinna	Cuba	US/Alaska
Brazil/Acre	Egypt	US/Aleutian
Brazil/DeNoronha	Europe/Central	US/Arizona
Brazil/East	Europe/Eastern	US/Central
Brazil/West	Europe/Western	US/Eastern
Canada/Atlantic	GB-Erie	US/Hawaii
Canada/Central	GMT	US/Indiana
Canada/Eastern	Iran	US/Mountain
Canada/East-Saskatchewan	Israel	US/Pacific
Canada/Mountain	Japan	US/Samoa
Canada/Newfoundland	Korea	
Local Time/Date – Enter the time in *hh.mm* format (am or pm). Enter the date in *mm/dd/yy* format. All DSL cards are Y2K compliant.		
Client NTP Mode – Broadcast/Unicast (Default = Broadcast). Select the Client Network Time Protocol Mode.		
NTP Server – *nnn.nnn.nnn.nnn* format. Enter the NTP Server IP address.		
Synchronized (hrs) – 1–24 (Default = 1). Enter the hours between synchronization.		
NVRAM Clear		**A-A-D**
Gives you the ability to clear out the Non-Volatile RAM (NVRAM) in order to reuse the card or to reconfigure the current card. A warning message appears if you attempt to reset the MCC card while others users are currently accessing the chassis. CAUTION: If you select yes on this screen, you permanently remove most of the configuration information and all IP addresses and routing tables will have to be reentered. The system performs a reset and returns to the factory configuration.		

Table 4-2. Card Status Menu Options (3 of 4)

NVRAM Config Loader	**A-A-E**
Gives you the ability to upload or download a copy of the card's binary configuration data to or from a Trivial File Transfer Protocol (TFTP) server. **Configuration File Name** – The file name may be a path name of directories separated by a forward slash (/) ending with the file name. The total path name length must be less than 40 characters. Specify the slot directory name (for example, slot_9/slot_9.cfg) if the file is to be stored in the card flash device. If the TFTP server is hosted by a DOS machine running other than Windows 2000 or Windows NT, then directory and file names must follow the 8.3 DOS naming convention. **DOS Machine** If your server is hosted by a DOS machine, you must name the file to be uploaded using the DOS convention 8-character length. The system automatically uploads the configuration file and creates directories and file names as needed. **UNIX Machine** If your server is hosted by a UNIX machine, the configuration file you name **is not** created on the UNIX system by the TFTP server. It is **critical** that you work with your system administrator to plan naming conventions for directories, file names, and permissions so that anyone using the system has read and write permissions. (This is a UNIX system security feature.) NOTE: This must be done before you can upload files to a UNIX server. **TFTP Server** – *Host name* (with DNS entry) or IP address *(nnn.nnn.nnn.nnn)* format. **TFTP Transfer Direction** – Upload/Download (Default = Upload). Select Upload to store a copy of the card's configuration on the server. Select Download to have the file server send a copy of the stored configuration file to the card. **Start Transfer** – Yes/No (Default = No). Displays after transfer: **Statistics:** **Packets Sent** – Number of packets sent in download. **Packets Received** – Number of packets received in download. **Bytes Sent** – Number of bytes sent in download. **Bytes Received** – Number of bytes received in download. **Transfer Time** – The length of time the transfer is taking. **Status** – The progress of the transfer. NOTE: After a download, the MCC card must be reset for the new configuration to take effect.	
Card Reset	**A-A-F**
Gives you the ability to reset the cards. This resets all counters to zero. If a new configuration or software version has been downloaded, the new code becomes active. **Reset Card** – Enter Yes to reset card. NOTE: This action disrupts the data flow for at least 10 seconds. A warning message appears if you attempt to reset the MCC card while others users are currently accessing the chassis.	

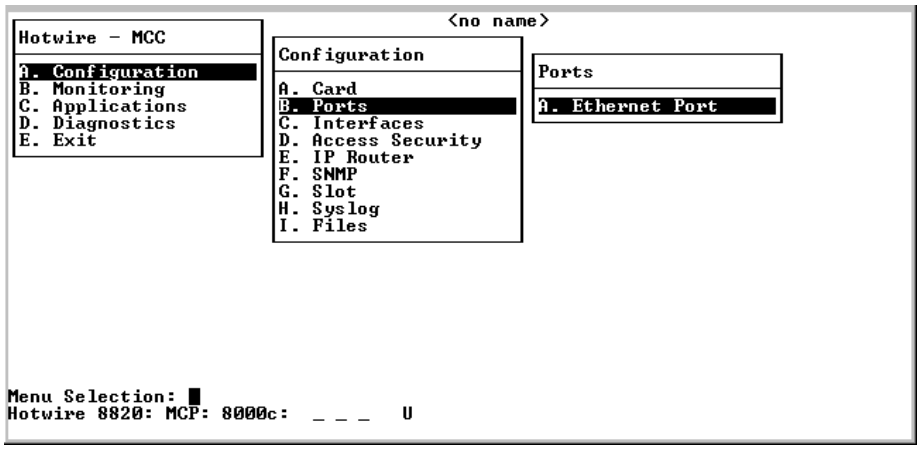
Table 4-2. Card Status Menu Options (4 of 4)

Download Code (Download Code and Apply Download)	**A-A-G**
Gives you the ability to download a new version of code and apply the downloaded code. See Appendix A, *Upgrade Procedures*, for more information on this feature.	
Download Code	**A**
This screen is similar to the NVRAM Config Loader screen. **Download Type** – MCC, SCM, PC, or SN. Identifies the system to be downloaded. You can start a download to a DSL router by typing its slot and port number. **Card/Slot #** – Number of card or slot to receive the download (1–18, A, B). NOTE: This field only appears if the chosen download type is PC (port card) or SN. Older versions of cards may not be compatible with this download feature. **SN Connected to Port #** – Enter port number 1–24. NOTE: This field only appears if the download type is SN. When you are downloading to an SN, service is disrupted until the download completes. **Immediate Apply** – Yes/No. The field is only an option if the Download Type is MCC. This field is not an option if the Download Type is SN. Answering yes in this field makes the port card or MCC card automatically reset upon completion. Answering no downloads new firmware to the card's ROM, but does not reset the card. It still executes from previous code stored in RAM. **Image File Name** – The file name may be a regular path name separated by a forward slash (/) ending with the file name. The total path name length must be less than 40 characters. If the TFTP server is hosted by a DOS machine, then directory and file names must follow the 8.3 naming convention imposed by DOS. **TFTP Server** – Enter the TFTP server address or a configured host name if an external TFTP server is used (*nnn.nnn.nnn.nnn* format). Enter M1 if the configuration file is stored in the on-card flash device. **Start Transfer** – Yes/No (Default = No). A warning message appears if you attempt to reset the MCC card while others users are currently accessing the chassis. Displays after transfer: **Statistics:** **Packets Sent** – Number of packets sent in download. **Packets Received** – Number of packets received in download. **Bytes Sent** – Number of bytes sent in download. **Bytes Received** – Number of bytes received in download. **Transfer Time** – The length of time the transfer is taking. **Status** – The progress of the transfer. Once the download is complete, press Ctrl-z to exit back to the Download Code submenu and select Apply Download.	
Apply Download (Reset System)	**B**
This selection applies the downloaded code and drops all connections by performing a device reset to the MCC card. This screen is used to overlay the previously downloaded image for the card. If you select yes at the **`Reset System`** prompt, the system goes through a system restart and interrupts service on the card. NOTE: If you have not downloaded code or if you selected yes for Immediate Apply, you cannot access this selection.	

Ports Menu

For Ethernet Port menu options, refer to Table 4-3, Ports Menu Options. To access the Ports menu, follow this menu selection sequence:

MCC Main Menu→*Configuration*→*Ports*→*Ethernet Port* (**A-B-A**)



The Ports menu provides one selection: Ethernet Port.

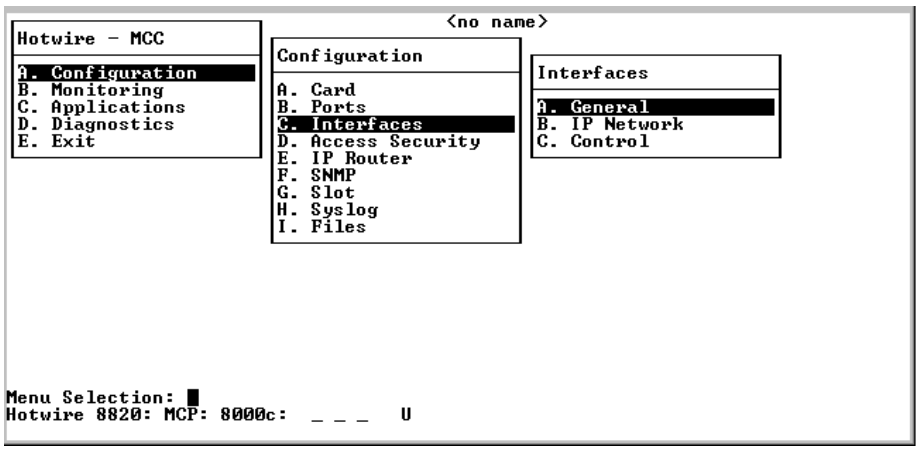
Table 4-3. Ports Menu Options

Ethernet Port	**A-B-A**
Gives you the ability to reset and configure the specified Ethernet port (e1a). **Port Name** – Enter e1a for the Ethernet port. **Full Duplex** – Enable/ Disable. Enable for Full Duplex mode, Disable for Half-Duplex mode (Default = Disable). NOTE: Full Duplex is not supported when Management Port Type is set to Internal. **Management Port Type** – Internal/External. Defaults to External (10BaseT) for all chassis. On the Hotwire 8820 GranDSLAM chassis, the Internal selection connects the Management port to the SCM card or TDM card that supports inband management. Select Internal only when you have logged on via the console port and the MCP has determined that there is an SCM or TDM card present that supports inband management (for Hotwire 8820 GranDSLAM chassis only). See Appendix E, *Simple Network Management Protocol*, for more information about network management. **Management Port Card/Slot #** – Enter the slot number of the TDM port card or SCM card that will provide the inband management channel for the DSLAM (Default = A for SCM). You must reset the MCC card for this change to take effect. NOTE: Management Port Card/Slot # only appears when Management Port Type is set to Internal. **Action** – Edit/Reset. Select Edit to configure the port. Select Reset to have changes become active. If Reset is selected without changes having been made to the Management Port Type or Management Port Card/Slot # fields, then only the Ethernet port resets. Otherwise, the MCC card resets.	

Interfaces Menu

To access the Interfaces menu, follow this menu selection sequence:

MCC Main Menu→*Configuration*→*Interfaces* (**A-C**)



The Interfaces menu provides the following selections:

- **A. General** – Configures several interface parameters.
- **B. IP Network** – Configures the MCC card interfaces.
- **C. Control** – Monitors, stops, and restarts the MCC card interfaces.

See Table 4-4, Interfaces Menu Options, for information about the options available from the Interfaces menu.

Obtaining General Interface Information and Changing MTU Value

Use the General Interfaces screen to obtain basic information about the e1a interface, and to change the Maximum Transmission Unit (MTU) value.

▶ Procedure

To enter card-level information:

1. Follow this menu selection sequence:

   Configuration→ *Interfaces*→ *General* (**A-C-A**)

   The Interfaces screen appears. See Table 4-4, Interfaces Menu Options.

2. Type **e1a** (for the Ethernet port interface) at the **`Interface Name:`** prompt and press Enter.

   The system displays the information listed in Table 4-4, Interfaces Menu Options.

3. For e1a, specify the desired maximum MTU value. If you change the default value, make sure the number is appropriate to your network.

4. Press Ctrl-z to save the changes and return to the Interfaces menu.

Configuring IP Addresses for the e1a Port

This screen allows you to configure up to 16 IP addresses for the e1a port. However, under normal conditions only one IP address in the management domain needs to be assigned.

▶ Procedure

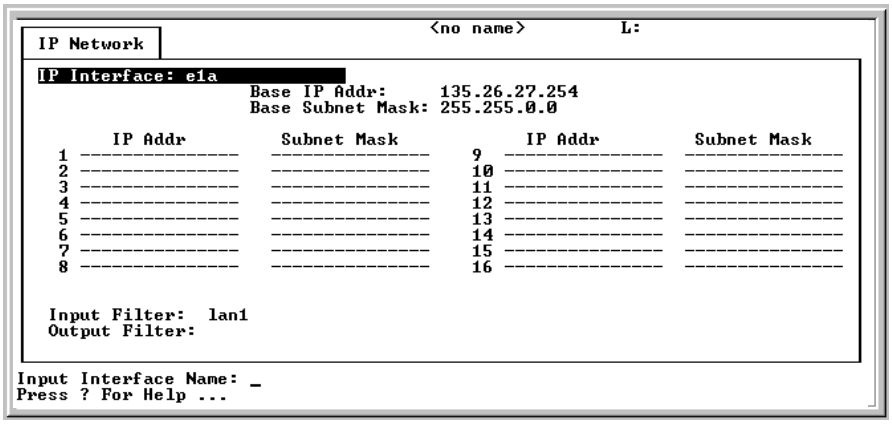
To configure the IP address for the e1a port:

1. Follow this menu selection sequence:

   Configuration→ *Interfaces*→ *IP Network* (**A-C-B**)

   The IP Network screen appears and displays the information listed in Table 4-4, Interfaces Menu Options.

2. Enter the IP interface name (must enter **e1a**). The following screen appears:


<no name> L:
IP Network
IP Interface: e1a
Base IP Addr: 135.26.27.254
Base Subnet Mask: 255.255.0.0
IP Addr Subnet Mask IP Addr Subnet Mask
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
Input Filter: lan1
Output Filter:
Input Interface Name: _
Press ? For Help ...

3. Enter up to 16 IP addresses.
4. Press Ctrl-z to save the changes and return to the Interfaces menu.

NOTE:

For changes to take effect, you must either restart the interface or reset the MCC card.

Stopping, Starting, and Monitoring an Interface

The Control Interface screen allows you to restart, stop, and monitor the current state of an e1a interface.

▶ Procedure

To stop, start, or monitor an e1a interface:

1. Follow this menu selection sequence:

   Configuration→ *Interfaces*→ *Control* (**A-C-C**)

   The Control Interface screen appears.

2. Type one of the following in the **`Command (Restart/Stop/Monitor):`** prompt and press Enter:

   — **Restart** – To display an interface.

   — **Stop** – To stop an interface.

   — **Monitor** – To display statistics about the current state of an interface.

3. Type **e1a** at the **`Interface Name:`** prompt and press Enter.

   The screen is populated depending on your previous entry.

4. Press Ctrl-z to save the changes and return to the Interfaces menu.

Interfaces Menu Options

For Interfaces menu options, refer to Table 4-4, Interfaces Menu Options. To access the Interfaces menu, follow this menu selection sequence:

MCC Main Menu→ *Configuration*→ *Interfaces* (**A-C**)

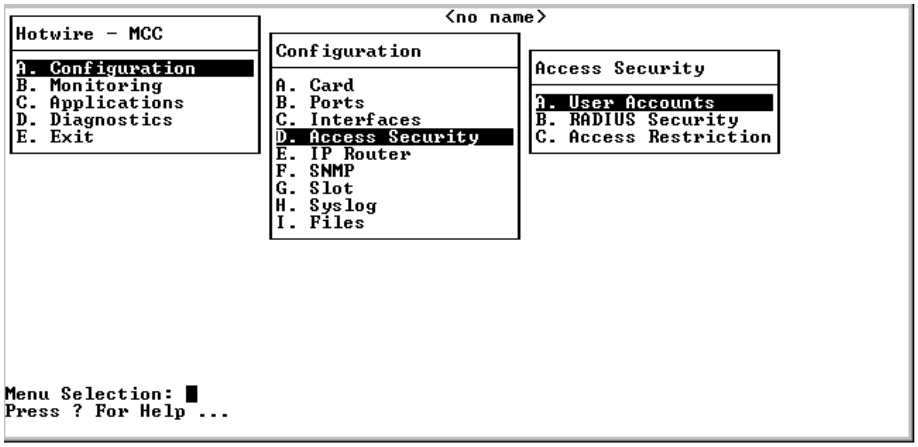
Table 4-4. Interfaces Menu Options

General (Interfaces)	**A-C-A**
Gives you the ability to configure basic information about a given interface. **Interface Name** – e1a = Ethernet port. **Type** – Static. Interface type. **Protocol** – Ether. Type of protocol for an interface. **Port list** – e1a. The name of the port associated with the Ethernet interface. NOTE: The MTU values are the only ones allowed on this screen. Make certain that if you change a default value, the numbers are appropriate to your network. Do a card reset or reset the interface. **MTU (max) (Maximum Transmission Unit)** – The range is 64–1600 (Default = 1536).	
IP Network	**A-C-B**
Allows you to configure up to 16 IP addresses for the e1a port. However, under normal conditions only one IP address in the management domain needs to be assigned. **IP Interface** – 15 characters. e1a = Ethernet port. **Base IP Addr** – *nnn.nnn.nnn.nnn* format. IP address for the e1a port. **Base Subnet Mask** – *nnn.nnn.nnn.nnn* format. IP address of the management domain subnet mask. **IP Addr** – IP address in *nnn.nnn.nnn.nnn* format. **Subnet Mask** – Subnet mask in *nnn.nnn.nnn.nnn* format. **Input Filter** – The filter that operates on inbound packets. Optional. **Output Filter** – The filter that operates on outbound packets. Optional. NOTES: – If you enter and save the name of a filter, either input or output, you bind the filter to the interface. If you delete a filter name, you delete the filter and its rules. – For changes to take effect, you must either restart the interface or reset the MCC card. – If you have made changes to this screen, you must do a card reset or restart the appropriate interface (except for changes to filters).	
Control (Control Interface)	**A-C-C**
Gives you the ability to restart, stop, and monitor (up, down, or testing) the current state of an interface.	

Access Security Menu

To access the Security menu, follow this menu selection sequence:

Configuration→Access Security (**A-D**)



The Access Security menu provides the following selections:

- **A. User Accounts** – Configures login accounts for local terminal, Telnet, and FTP sessions. Up to 10 active users can be supported. Accounts can be added, edited, and deleted.
- **B. RADIUS Security** – Enables Radius Authentication for user logins.
- **C. Access Restriction** – Enables or disables Telnet, FTP, and SNMP access to the MCC Ethernet port and inband management PVC, and provides a security check of the originating IP address. When enabled, the MCC matches the source address of a Telnet, FTP, and SNMP message against its list of approved management hosts.

See Table 4-5, Access Security Menu Options, for information about options available from the Access Security menu.

Adding, Changing, and Deleting Users

The User Accounts screen allows you to add, edit, or delete a user from a system account. Also use this screen to edit user passwords and privileges.

User accounts provide security to users accessing the system from the VT100-compatible terminal interface and via Telnet over the LAN.

NOTE:

To prevent unauthorized access to the DSL system, it is important to set up accounts on the MCC card. If no accounts are set up, then no login or password is required to gain entry to the MCC card via the terminal interface or Telnet. This means that *anyone* can access the DSL system.

If you configure an account on the MCC card with Administrator privileges, that user account has Administrator privileges on the MCC card as well as on all DSL cards in the chassis.

▶ Procedure

To add, change, or delete a user:

1. Follow this menu selection sequence:

   Configuration→ *Access Security* → *User Accounts* (**A-D-A**)

   The User Accounts screen appears.

2. Type one of the following at the **`Action:`** prompt and press Enter:

   — **Add** – To add a user account.

   — **Edit** – To change an existing user account.

   — **Delete** – To remove an existing user account.

3. Type the desired user name (up to 15 characters) at the **`Login ID:`** prompt and press Enter. Enter up to 10 passwords, one per account.

   NOTE:

   At this prompt, press Ctrl-v to see a list of all user accounts.

4. Type the password (up to 15 characters) associated with the login ID at the **`Password:`** prompt and press Enter.

   NOTE:

   If you forget your password, contact our Technical Service Center. Have the serial number of the MCC card available, and the service representative will provide you with a password.

5. Retype the password at the **`Repeat Password:`** prompt and press Enter.

6. Type one of the following at the **`Privilege:`** prompt and press Enter:

   — **Operator** – For read-only access privilege.

   — **Administrator** – For complete system access privilege.

7. Press Ctrl-z to save the changes and return to the Access Security menu.

Enabling and Disabling RADIUS Authentication

RADIUS Authentication allows for passwords to be centrally administered. You must have at least one local Administrator account for RADIUS Authentication to be configured. The addresses of up to four RADIUS servers can be configured. The user ID and password must be entered into each of those servers.

The RADIUS server must be configured to match the RADIUS information configured on the MCC. If the RADIUS server configuration does not match that of the MCC, the MCC will deny the login request.

The following variables must be configured to match:

- **Network Access Server (NAS) IP Address** – Must match the Server IP Address.
- **NAS Port** – Must match the UDP Port number.
- **Secret** – Must match the Secret number.

The IP addresses of the RADIUS servers should be entered on the screen in priority order (most important first). If the MCC fails to connect with the first server, it tries again for the specified number of attempts. If the first server is not reached after the specified number of attempts, the MCC tries to connect with the second RADIUS server, then the third, then the fourth.

When you enter your user name and password, the local user account database is checked first. If a matching account is found, you are logged in. If no matching account is found, but the database contains no Administrator-level user accounts, you are still logged in. RADIUS Authentication is only used if the database contains an Administrator-level account and RADIUS Authentication has been enabled. A RADIUS Access-Request message is then created with the user inputs and is sent to the first of up to four configured RADIUS servers. Only the receipt of an Access-Accept message from a RADIUS server will allow you to be logged in. A port number is included in the Access-Request message that indicates whether you are using the console, Telnet (via the MCC's Ethernet port or the management PVC), or FTP to gain access.

▶ Procedure

To enable RADIUS Authentication:

1. Follow this menu selection sequence:

   Configuration→ *Access Security* → *RADIUS Security* (**A-D-B**)

   The RADIUS Check screen appears and the **`RADIUS Authentication:`** field is highlighted. See Table 4-5, Access Security Menu Options.

2. Type one of the following at the **`Enable/Disable:`** prompt and press Enter:

   — **Enable** – To enable RADIUS Authentication.

   — **Disable** – To disable RADIUS Authentication.

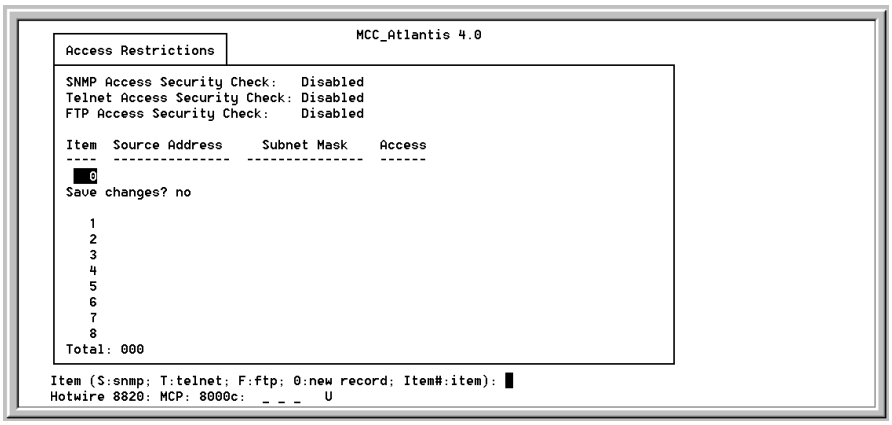
3. Enter the Server IP address at the **`IP Address <nnn.nnn.nnn.nnn> or space to delete:`** prompt.

4. Enter the UDP Port number at the **`Input Number:`** prompt.

5. Enter the RADIUS secret string at the **`Secret:`** prompt.
6. Enter the maximum response time of the RADIUS Server at the **`Timeout:`** prompt.
7. Enter the number of times the system should check the local user accounts at the **`Input Number:`** prompt.
8. Press Ctrl-z to save the changes and return to the Access Security menu.

Enabling and Disabling Telnet, FTP, and SNMP Access

You can enable or disable Telnet, FTP, and SNMP access on the Access Restrictions screen. When enabled, the MCC matches the source address of a Telnet, FTP, or SNMP message against the list of approved management hosts or approved subnets.



▶ Procedure

To enable Telnet and SNMP access security:

1. Follow this menu selection sequence:

   Configuration→ *Access Security* → *Access Restriction* (**A-D-C**)

   The Access Restriction screen appears

2. In the **`Telnet Access Security Check:`** field, type one of the following and press Enter:

   — **Enable** – To enable Telnet access security

   — **Disable** – To disable Telnet access security

3. In the **`SNMP Access Security Check:`** field, type one of the following and press Enter:

   — **Enable** – To enable SNMP access security

   — **Disable** – To disable SNMP access security

4. In the **`FTP Access Security Check:`** field, type one of the following and press Enter:

   — **Enable** – To enable FTP access security

   — **Disable** – To disable FTP access security

5. Enter up to 16 hosts or subnets that have permission to access the DSL system at the **`Source Addr`** prompt. Enter the corresponding subnet mask at the **`Subnet Mask`** prompt.

   To define a subnet entry, the IP address must be entered as the lower boundary address of the subnet. Otherwise, only a host entry can be configured (for example, a subnet with a mask of 255.255.255.192 requires one of the following IP addresses: 255.255.255.0, 255.255.255.64, 255.255.255. 128, or 255.255.255.192). For multiple users with IP addresses in the same subnet, enter both the IP address and the subnet mask in the *nnn.nnn.nnn.nnn* format.

   NOTE:

   To disable SNMP access to the DSL chassis, enable SNMP Access Security, but do not enter any host or subnet addresses. To disable Telnet Access Security to the DSL chassis, enable Telnet access, but do not enter any host or subnet addresses. To disable FTP Access Security to the DSL chassis, enable FTP access, but do not enter any host or subnet addresses.

6. Enter either T (for Telnet), S (for SNMP), or F (for FTP) at **`Item`** prompt to change access security settings.

7. Enter the access permissions at the **`Access`** prompt in the form of *xyz*.

   Where *x* =

   — **W** = SNMP read/write access

   — **R** = SNMP read-only access

   — **N** = No SNMP access

   Where *y* =

   — **T** = Telnet access

   — **N** = No Telnet access

   Where *z* =

   — **F** = FTP access

   — **N** = No FTP access

8. Press Ctrl-z to save the changes and return to the Access Security menu.

Access Security Menu Options

For Access Security menu options, refer to Table 4-5, Access Security Menu Options. To reach the Access Security menu, follow this menu selection sequence:

MCC Main Menu→ *Configuration*→ *Access Security* (**A-D**)

Table 4-5. Access Security Menu Options (1 of 2)

User Accounts	**A-D-A**
Gives you the ability to add, edit, or delete a user from a system account and to edit user passwords and privileges. Up to 10 active users can be supported. User accounts provide DSL system security by requiring anyone trying to log on to the system to have a valid password. User accounts on the MCC provide security to users accessing the system from the VT100-compatible terminal interface and via Telnet over the management domain LAN. If no accounts are set up, then no login or password is required to gain entry to the system via the terminal interface or Telnet. If you configure an account on the MCC card, you have privileges on both the MCC and DSL cards. **Action** – Add/Edit/Delete. **Login ID** – Enter your Login ID. **Password** – Enter the password associated with the login ID (15 characters maximum). **Repeat Password** – Reenter the password. **Privilege** – Operator/Administrator. Enter Operator for read-only access; enter Administrator for complete system access. NOTE: Press Ctrl-v to see a list of all user accounts at the Login ID prompt.	
RADIUS Security	**A-D-B**
Gives you the ability to enable RADIUS Authentication for user logins. The DSL system requires at least one local Administrator account for RADIUS Authentication to be in effect. The system checks against local user accounts before it sends the request to the RADIUS server. The RADIUS server entries should be entered in order of priority. **RADIUS Authentication** – Enabled/Disabled (Default = Disabled). **Server IP Address** – Enter the RADIUS server IP address in *nnn.nnn.nnn.nnn* format. Up to four server addresses can be entered. **UDP Port** – Enter the User Datagram Protocol (UDP) port number used by RADIUS – 1–65535 (Default = 1812). **Secret** – Enter the RADIUS secret string (6–32 characters). **Timeout** – Enter the maximum response time of the RADIUS server: 3–30 seconds (Default = 10). **Attempts** – Enter the number of times that the system checks the local user accounts: 1–3 (Default = 3).	

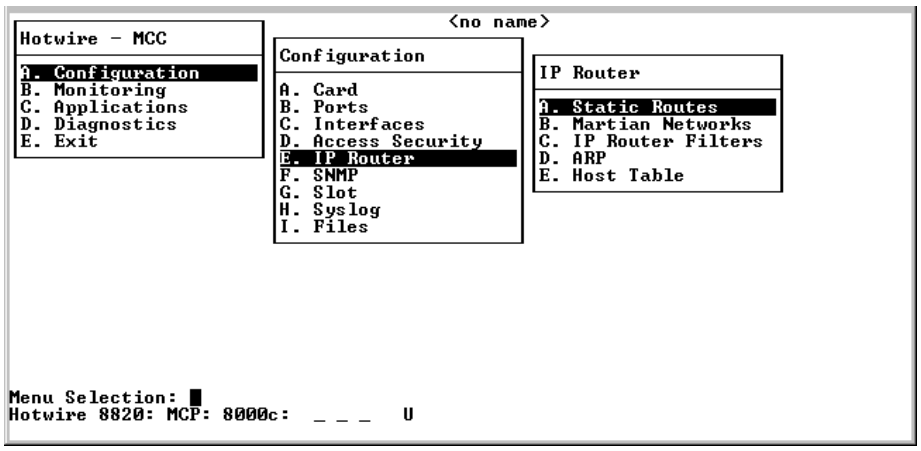
Table 4-5. Access Security Menu Options (2 of 2)

Access Restriction	A-D-C
Gives you the ability to enable or disable the Telnet/FTP/SNMP access to the MCC using the Ethernet port (out of band) or management PVC (inband). When enabled, the MCC matches the source address of a Telnet/FTP/SNMP message against its list of approved management hosts. **SNMP Access Security Check** – Enabled/Disabled (Default = Disabled). When enabled, the DSL system only accepts SNMP messages from an SNMP manager whose IP address matches an IP address or subnet entry on this screen. When disabled, SNMP messages are accepted from any source. If you enable Telnet and there are no entries in the table, then access is denied. **Telnet Access Security Check** – Enabled/Disabled (Default = Disabled). When enabled, the DSL system only accepts Telnet sessions from a host whose IP address matches an IP address or subnet entry on this screen. When disabled, Telnet sessions are accepted from any source. If you enable Telnet and there are no entries in the table, then access is denied. **FTP Access Security Check** (Default = Disabled). When enabled, the DSL system only accepts FTP sessions from a host whose IP address matches an IP address or subnet entry on this screen. When disabled, FTP sessions are accepted from any source. If you enable FTP and there are no entries in the table, then access is denied. **Source Addr** – Enter up to 16 source addresses of NMS managers in *nnn.nnn.nnn.nnn* format. **Subnet Mask** – Enter up to 16 subnet masks of NMS managers in *nnn.nnn.nnn.nnn* format. (This is entered only if an entire subnet is to be granted access permission.) **Item** – Enter one of the following: – **T** to change Telnet Access Security Check settings – **S** to change SNMP Access Security Check settings – **F** to change FTP Access Security Check settings **Access** – Enter the permission granted to the NMS manager in the form of *xyz*. Where *x* = – **W** = SNMP (read/write) access – **R** = SNMP (read-only) access – **N** = No SNMP access (Although on the approved list, this host has no access to the DSL system.) Where *y* = – **T** = Telnet access – **N** = No Telnet access (Although on the approved list, this host has no access to the DSL system.) Where *z* = – **F** = FTP access – **N** = No FTP access (Although on the approved list, this host has no access to the DSL system.)	

IP Router Menu

To access the IP Router menu, follow this menu selection sequence:

Configuration→*IP Router* (**A-E**)



The IP Router menu provides the following selections:

- **A. Static Routes** – Configures static routes to protocols and filters.
- **B. Martian Networks** – Restricts routing information from certain sources.
- **C. IP Router Filters** – Provides an overview of the various filters in the system. Use the IP Filter Configuration screen to add, edit, and delete filters.
- **D. ARP** – Configures general Address Resolution Protocol (ARP) cache parameters, adds entries into the ARP cache, and deletes entries line by line in the ARP cache.
- **E. Host Table** – Defines mappings between IP addresses and host names.

See Table 4-6, IP Router Menu Options, for information about the options available from the IP Router menu.

Adding and Deleting Static Routes

The Static Routes screen allows you to add or delete static routes in the system. You can add up to 32 static routes.

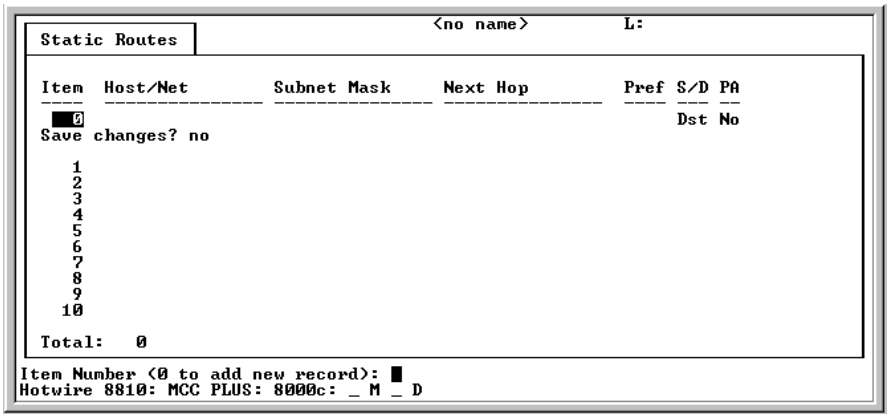
▶ Procedure

To configure static routes:

1. Follow this menu sequence:

   Configuration→ *IP Router* → *Static Routes* (**A-E-A**)

   The Static Routes screen appears.



2. Enter an item number or type **0** (zero) at the **`Item (0 to add new record):`** prompt.
3. Do one of the following at the **`Host/Net (or space to delete route):`** prompt.
   - — Type the host or network address (in *nnn.nnn.nnn.nnn* format) to add an entry.
   - — Type spaces to delete an entry.
4. Type the desired value in the fields and press Enter. See Table 4-6, IP Router Menu Options.

   When all entries are made, the **`save changes`** field is highlighted and the **`yes/no:`** prompt appears. Type the desired response.
5. Press Ctrl-z to return to the IP Router menu.

The following table lists error messages that may appear on the Static Routes screen.

Message	Description
Routing Table: Route not added	Route was saved into NVRAM but not added to the active routing table.
Routing Table: Route limit reached for routing table	Route was saved into NVRAM but not added to the active routing table because the active routing table is full.
Routing Table: Next hop gateway currently unreachable	Route was saved into NVRAM but not added to the active routing table because there is no way to reach the next hop gateway. If an interface comes up that has the next hop gateway, the route is added.
Routing NVRAM: Database Error	Route was not saved into NVRAM and not added to the active table. This is a general database error.
Routing NVRAM: Database Route Limit Reached	Route was not saved into NVRAM and not added to the active table because the NVRAM is full.

Adding and Deleting Martian Networks

Martian Networks allow you to create a list of specific IP addresses from which the MCC card **will not accept** any packets from those addresses.

NOTE:

The system is shipped with default Martian Networks labeled “(fixed).” Do not remove these Martian Networks.

▶ Procedure

To display Martian Networks information:

1. Follow this menu sequence:

   Configuration→ *IP Route*r → *Martian Networks* (**A-E-B**)

   The Martian Networks screen appears. See Table 4-6, IP Router Menu Options.

2. Press Enter or type **0** (zero) to add an entry in the Item field. (Enter the item number to edit or delete an entry.)

3. Enter the address of the unwanted source at the Martian Network ID at the **`Martian ID (or space to delete route):`** prompt. (Enter a different network ID to edit the field, enter a space to delete the field.)

4. Enter the new Martian Net Mask ID at the **`nnn.nnn.nnn.nnn:`** prompt. (Enter a different Martian mask ID to edit the field, enter a space to delete the field).

5. Enter **yes** at the **`yes/no`** prompt to save the changes.

NOTE:

The card must be reset for the changes to take effect.

Adding, Changing, and Deleting Filters

The Access Security screen (**A-D-C**) provides a set of access filters for Telnet, FTP, and SNMP packets. See *Enabling and Disabling Telnet, FTP, and SNMP Access* on page 4-22. If other types of IP traffic must also be filtered, then use the IP Filter Table screen (**A-E-C**).

Use the Filter Table screen to display an overview of the various filters in the system. Use the IP Router Filters configuration screen to add, edit, and delete filters.

A filter is a rule (or set of rules) applied to an e1a interface to indicate whether a packet can be forwarded or discarded. You can add, edit, or delete filter rules within a named set. Use the IP Filter Configuration screen to build named sets of filter rules. Press Ctrl-v to view existing filter names.

A filter successively applies its rules to the information in the packet header until a match is found. The filter then performs the action specified by the rule on that packet: forward or discard.

NOTES:

— Rules apply to source and destination ports on the MCC. There may be up to 33 rules per filter, but the greater number of rules, the lesser the performance of the MCC.

— A maximum of two filters can be configured on the MCC card.

▶ Procedure

To display filter information:

1. Follow this menu sequence:

   Configuration → *IP Router* → *IP Router Filters* (**A-E-C**)

   The Filter Table screen appears. See Table 4-6, IP Router Menu Options.

2. At the **`Input Number:`** prompt, do one of the following:

   — Type **0** to add a new filter to existing filters and press Enter.

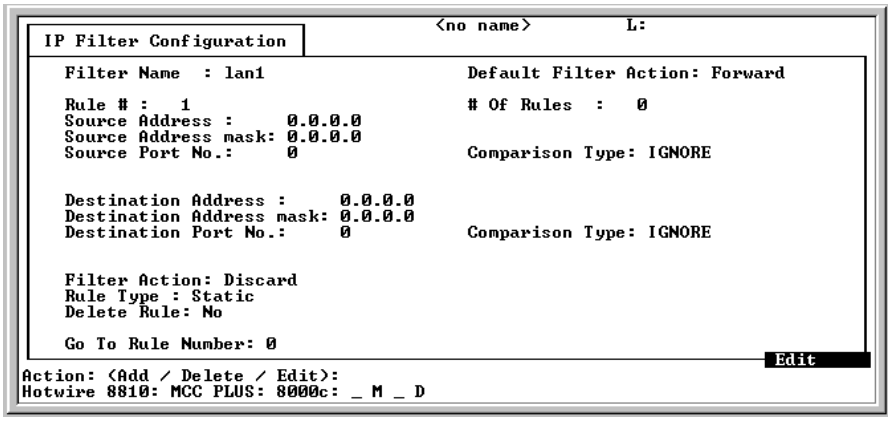
   The Add selection takes you to the IP Filter Configuration screen. When you exit that screen, you return to the Filter Table screen.

   — Type the number of the line of the filter you want to edit. Press Enter.

   The IP Filter Configuration screen appears. When you exit that screen, you return to the Filter Table screen.

   — Type the number of the line of the filter you want to delete. Press Enter.

   The system deletes the selected filter.



3. Press Ctrl-z and type **yes** at the **`Save (yes/no)`** prompt to save the changes and return to the IP Router menu.

NOTE:

The card must be reset for the changes to take effect.

Using the ARP Submenu Options

Use the ARP submenu to configure general Address Resolution Protocol (ARP) cache parameters, add entries to the ARP cache, and delete entries line by line in the ARP cache.

▶ Procedure

To configure ARP cache parameters:

1. Follow this menu sequence:

   Configuration → *IP Router* → *ARP* → *Parameters* (**A-E-D-A**)

   The ARP Parameters screen appears.

2. Type values in the fields and press Enter. See Table Table 4-6, IP Router Menu Options.

3. Press Ctrl-z and type **yes** at the **`Save (yes/no)`** prompt to save the changes and return to the ARP menu.

   NOTE:

   The card must be reset for the changes to take effect.

▶ Procedure

To add ARP cache entries:

NOTE:

Only permanent (PERM) entries are stored in non-volatile (NV) memory. All other entries added to the ARP cache are lost when you reset the card.

1. Follow this menu sequence:

   Configuration → *IP Router* → *ARP* → *ARP Entry* (**A-E-D-B**)

   The Add ARP Entry screen appears.

2. At the **`Item Number (0 to add new record):`** prompt, enter the value for the desired action.

3. Type values in the fields (or accept the default values) and press Enter. See Table 4-6, IP Router Menu Options.

4. When you complete your entries, the Save Changes? field is highlighted and the **`yes/no`** prompt appears at the bottom of the screen. Type **y** to save the changes, **n** to discard the changes.

5. The **`Item (0 to add new record):`** prompt appears. Press Ctrl-z to return to the ARP menu.

   The system displays the ARP menu.

   NOTE:

   The card must be reset for the changes to take effect.

Mapping IP Addresses and Host Names

Use the IP Host Table screen to define mappings between IP addresses and host names. The host table holds the host-name-to-IP-address translation for Telnet sessions from the card as well as other functions. The table allows you to connect to foreign hosts by name rather than by IP address.

An alternative to populating this table is to define a DNS server. See *Configuring Access to DNS Servers* on page 4-4 for more information.

▶ Procedure

To configure static routes host names:

1. Follow this menu sequence:

   Configuration → *IP Router* → *Host Table* (**A-E-E**)

   The IP Host Table screen appears. See Table 4-6, IP Router Menu Options.

2. Type the IP address at the *nnn.nnn.nnn.nnn* prompt and press Enter.
3. Type the host name in *nnn.nnn.nnn.nnn* format at the **`Host Name:`** prompt and press Enter.
4. Press Ctrl-z to save the changes and return to the IP Router menu.

Table 4-6. IP Router Menu Options (1 of 3)

Static Routes	**A-E-A**
Gives you the ability to add or delete static routes in the system. You can add up to 32 static routes. **Item** – Press Enter or enter 0 (zero) to add entry. **Host/Net** – *nnn.nnn.nnn.nnn* format or space to delete entry. **Subnet Mask** – Associated subnet mask for the specified destination IP address. This field is read-only for dynamic routes. **Next Hop** – *nnn.nnn.nnn.nnn* format. **Pref** – How preferable one route is to another, if two routes go to the same destination. (The lower the number, the more preferable.) **S/D** (Source/Destination) – Source or destination IP address of the packet. **PA** (Proxy ARP) – Router answers ARP requests intended for another machine. NOTE: When you define a source route, the Proxy ARP field is not selectable.	
Martian Networks	**A-E-B**
Gives you the ability to enter addresses that the system recognizes as invalid. **Item** – Press Enter or type 0 to add entry. **Martian Net ID** – *nnn.nnn.nnn.nnn* format or space to delete entry. Enter IP address of unwanted source. **Martian Net Mask** – *nnn.nnn.nnn.nnn* format. Enter IP mask of unwanted source. NOTE: The system is shipped with default Martian Networks. It is recommended that you do not remove entries. If you make changes to this screen, you must do a card reset.	
IP Router Filters	**A-E-C**
The IP Filter Table screen displays the following information: **Line** – Enter a value from 1–8 to add, delete, or modify individual filter entries. **Filter Name** – Name of the IP filter. (This field is read-only.) **# of Static Rules** – Number of static rules in filter. (This field is read-only.) **# of Dynamic Rules** – For future use. **Ref Cnt** – Number of active interfaces using the filter. (This field is read-only.) **Def Action** – Forward/Discard. Default action for the filter. (This field is read-only.) ■ Select 0 (zero) to add a new filter. ■ Select # (*n*) to edit existing filters. Example: Enter 3 to add Filter #3. ■ Select –# (–*n*) to delete a filter. Example: Enter –6 to delete Filter #6. The Add or Edit selection takes you to the IP Filter Configuration screen. When you exit that screen, you return to the IP Filters screen. NOTE: Deleting the filter deletes all the rules associated with that filter.	

Table 4-6. IP Router Menu Options (2 of 3)

IP Filters (IP Filter Configuration screen)	A-E-C

Allows you to build multiple rules for an IP filter. A filter consists of a set of rules applied to a specific interface to indicate whether a packet received or sent out of that interface is forwarded or discarded. You can add, edit, or delete filter rules within a named set.

A filter works by successively applying the rules to the information obtained from the packet header until a match is found. The filter then performs the action specified by the rule on that packet, which forwards or discards the packet. If all the rules are searched and no match is found, the configured default filter action is executed.

Host rules have higher precedence than network rules. Rules apply to the source/destination IP address and source/destination port number. You can have up to 33 rules per filter. Each rule reduces the packet throughput of the DSL card.

NOTE: There can be two filters per MCC card, one input filter and one output filter. Once rules have been configured, you can then bind and activate the filter on the MCC interface using the *Configuration→ Interfaces → IP Network* screen (**A-C-B**). See Table 4-4, Interfaces Menu Options.

Filter Name – Up to 12 characters.

Default Filter Action – Forward (Packet)/Discard (Packet) (Default = Forward). The Default Filter Action applies when there is no match or the filter has no rules configured.

Rule # – Up to 33 rules can be configured for each filter. The rule number is automatically assigned. The rules are reviewed sequentially. Enter the most common rules first.

 # Of Rules – The number of rules that apply to this port.

Source Address – *nnn.nnn.nnn.nnn* format. Enter valid host or network IP address. If 0.0.0.0 is entered, Source Comparison is ignored. For additional information, refer to *Configuring Subnet Masks* in the *Hotwire MVL, ReachDSL, RADSL, IDSL, and SDSL Cards, Models 8310, 8312/8314, 8510/8373/8374, 8303/8304, and 8343/8344, User's Guide*.

Source Address mask – *nnn.nnn.nnn.nnn* format. If you specify a source subnet mask of 0.0.0.0, the system skips the source address comparison.

Source Port No. – 0–65535 (Default = 0).

Comparison Type (for source information) (Default = Ignore). Type of comparison to be done on the source port number specified in the packet and rule:

- Ignore – Ignore ports. Do not do a comparison.
- EQ – Equal to. Do a comparison when the port number in the rule is *equal to* the port number in the packet.
- NEQ – Not Equal to. Do a comparison when the port number in the rule *is not equal* to the port number in the packet.
- GT – Greater than. Do a comparison when the port number in the rule *is greater than* the port number in the packet.
- LT – Less than. Do a comparison when the port number in the rule *is less than* the port number in the packet.
- In_Range – Within the specified range. Do a comparison when the port number in the packet is *within* the specified range.
- Out_Range – Outside of the specified range. Do a comparison when the port number in the packet is *outside* the specified range.

Max. Source Port No – 0–65535. Appears only when the source comparison type is In_Range or Out_Range.

Destination Address – *nnn.nnn.nnn.nnn* format.

(Continued on next page)

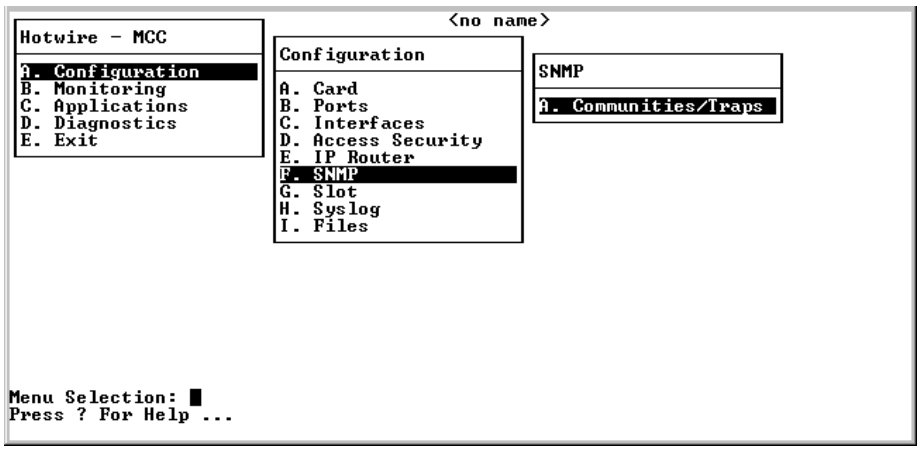
Table 4-6. IP Router Menu Options (3 of 3)

IP Filters (IP Filter Configuration screen) (*continued*) **A-E-C**
Destination Address mask – *nnn.nnn.nnn.nnn* format. If you specify a destination subnet mask of 0.0.0.0, the system skips the destination address comparison. **Destination Port No.** – 0–65535 (Default = null). **Comparison Type** (for destination information) – Same values as Comparison Type for source information (above). **Max. Destination Port No.** – 2–65535. Appears only when the destination port comparison type is In_Range or Out_Range. **Filter Action** – For a rule, TCP, UDP, or ICMP traffic will be forwarded or discarded provided other conditions have been satisfied. **Rule Type** – Static or Dynamic. **Delete Rule** – Yes/No (Default = No). **Go to Rule Number**– Yes/No (Default = No).
ARP (Parameters, ARP Entry) **A-E-D**
Parameters (A)
Allows you to configure general Address Resolution Protocol (ARP) cache parameters. **Complete Entry Timeout (minutes)** – 1–200,000 (Default = 20). **Incomplete Entry Timeout (minutes)** – 1–200,000 (Default = 3). **Default Route Entry Timeout (minutes)** – 1–20 NOTE: If you have made changes to this screen, you must do a card reset. **Add Entry?** – Enter Yes to add entry. **Add Another Entry?** – Enter Yes to add another entry.
Add ARP Entry (B)
Gives you the ability to add entries to the ARP cache. **Item** – Item number. **IP Address** – *nnn.nnn.nnn.nnn* format. **MAC Address** – *xx-xx-xx-xx-xx-xx* format. **VNID** – VNID number. **Trailer** – Control data appended to a packet. Yes/No (Default = No). **Perm** – Yes/No (Default = No). If you select yes for Perm and no to proxy, the ARP entry is saved in NVRAM (up to 32 entries; 8 for the MCC). These are loaded when the card reboots.
Host Table (IP Host Table) **A-E-E**
Allows you to define mappings between IP addresses and host names. The host table holds the host name-to-IP-address translation for Telnet sessions from the card. An alternative to populating this table is to define a DNS server (see *DNS Setup A-A-B* on page 4-9). Enter the IP Address and host name in *nnn.nnn.nnn.nnn* format. Press Enter after each entry. NOTE: You must confirm the save for any changes to take effect**.**

SNMP Menu

To access the SNMP menu, follow this menu selection sequence:

Configuration → *SNMP* (**A-F**)



The SNMP menu provides one selection: Communities/Traps.

Defining a Community and Enabling Traps

The SNMP Communities/Traps screen has three functions:

- Enables/Disables the Authentication Failure Trap mechanism
- Stores SNMP Community String names
- Stores NMS host IP addresses to which trap messages are sent

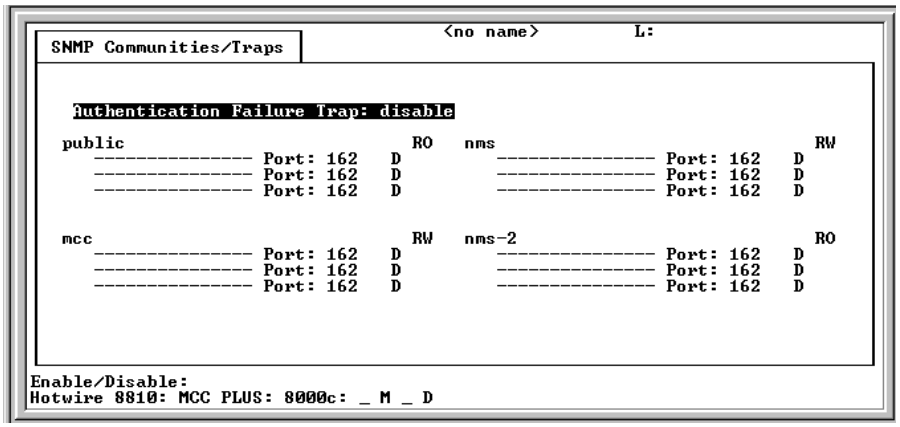
The SNMP Communities/Traps screen allows you to enable or disable the Authentication Failure Trap mechanism and define a community by specifying the SNMP NMS manager that receives the traps. Community strings define managers for all cards in the chassis. Up to three managers can be assigned for each community. You can also enable or disable the generation of *all* traps.

▶ Procedure

1. Follow the menu selection sequence:

   Configuration → *SNMP* → *Communities/Traps* (**A-F-A**)

   The SNMP Communities/Traps screen appears with the **`Authentication Failure Trap:`** field highlighted. Your response at the prompt determines whether the Authentication Failure Trap mechanism is enabled or disabled on the MCC. See Table 4-7, SNMP Menu Options.


<no name> L:
SNMP Communities/Traps
Authentication Failure Trap: disable
public RO nms RW
Port: 162 D Port: 162 D
Port: 162 D Port: 162 D
Port: 162 D Port: 162 D
mcc RW nms-2 RO
Port: 162 D Port: 162 D
Port: 162 D Port: 162 D
Port: 162 D Port: 162 D
Enable/Disable:
Hotwire 8810: MCC PLUS: 8000c: _ M _ D

2. Type your response at the **Enable/Disable:** prompt and press Enter.

   The first community string field is highlighted (default name: public). This community string has read-only permission.

3. Press Enter to accept the default name, or type a different community string name at the **Community Name:** prompt and press Enter.

   The permissions field is now highlighted.

4. Press Enter to accept the default (read-only) permission for this community string or change the permission at the prompt and press Enter.

   The IP address field is highlighted. This is the IP address of the NMS manager to which SNMP traps are sent.

5. Type the IP address of the NMS manager(s) at the **IP Address nnn.nnn.nnn.nnn (or space to delete):** prompt and press Enter.

   The Port Input Number field is highlighted.

6. Enter the port number at the **Input Number:** prompt and press Enter.

   The Enable/Disable field is highlighted. This field determines whether *any* trap messages are sent to the specified destination.

7. Type your response at the **Enable/Disable:** prompt and press Enter.

   The second IP Address field is highlighted.

8. Press Ctrl-z and the **Configuration has been modified. Save (yes/no):** prompt appears. Enter your desired response.

You have established Authentication Trap Failure security on the MCC.

You can repeat the procedures and create different levels of security for other IP addresses within the same community string and for other community strings.

SNMP Menu Options

For SNMP menu options, refer to Table 4-7, SNMP Menu Options. To access the SNMP menu, follow this menu selection sequence:

MCC Main Menu → *Configuration* → *SNMP* (**A-F**)

See Appendix E, *Simple Network Management Protocol*, for more information.

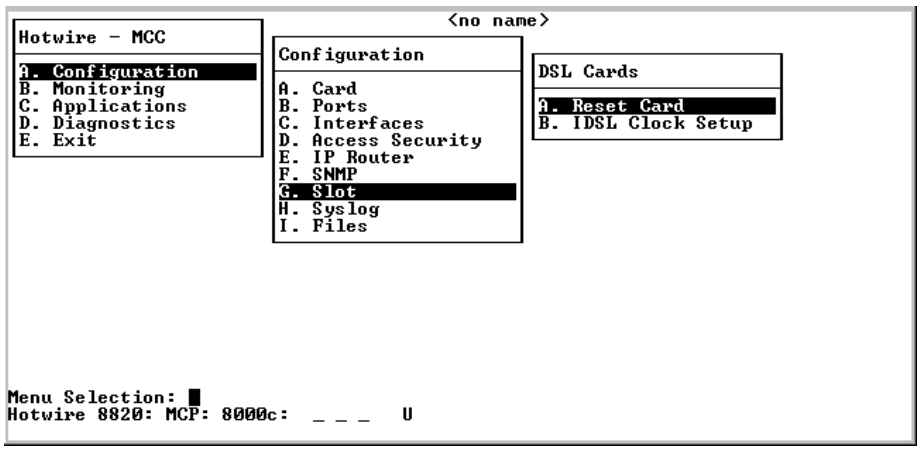
Table 4-7. SNMP Menu Options

Communities/Traps (SNMP Communities/Traps)	**A-F-A**
Lets you enable the Authentication Failure Trap Mechanism, store SNMP Community string names for the DSL card, and store trap addresses. It also lets you configure four communities with three trap destinations each. **Authentication Failure Trap** – Enable to send a trap when the community string of an SNMP request does not match table entry or when the password for a Telnet session or local access is incorrect. **Community Name** – 32 characters, up to four unique entries per screen. Default names are public (ro), mcc (rw), nms (rw), nms-2 (ro). **Access** – Read-Only(ro)/ReadWrite(rw)/NoAccess(na), up to four entries per screen. **IP Address** – To send traps to up to three addresses per community name, use the *nnn.nnn.nnn.nnn* format. Enter NMS system host address. **Port** – *nnn* format. Enter NMS system port number. **Send Traps** – Set to E to Enable traps to be sent to this address. Set to D to disable.	

Slot (DSL Cards) Menu

To access the DSL Cards menu, follow this menu selection sequence:

Configuration → *Slot* (**A-G**)



The DSL Cards menu provides the following selections:.

- **A. Reset Card** – Resets the DSL card in the selected slot.
- **B. IDSL Clock Setup** – Configures the clock mode for the selected IDSL card.

See Table 4-8, Slot (DSL Cards) Menu Options, for information about the options available from the DSL Card menu.

Resetting a Slot

Use the Reset Slot screen to reset a DSL card in any slot. Perform a reset if a DSL card does not appear on either the Quick Card Select or Port Card Select screen.

▶ Procedure

To reset a DSL slot:

1. Follow this menu sequence:

   Configuration → *Slot* → *Reset Card* (**A-G-A**)

   The Reset Card screen appears.

2. Type the slot number of the DSL card at the **`Reset Card/Slot (nn or DSLnn):`** prompt.

3. Type one of the following commands:

   — **ForceBootP** – A nondisruptive reset that only works for cards with T1 and E1 connections.

   — **Reset** – A disruptive reset of less than 30 seconds.

4. Do one of the following at the **`Clear NVRAM`** prompt:

   — Type **no** to perform no action on the NVRAM. This is the default.

   — Type **yes** to clear non-volatile RAM.

   If you select **yes** on this screen, you permanently remove configuration information stored on this card. All IP addresses and routing tables will need to be reentered. The system performs a card reset and returns to factory settings.

   NOTE:

   This function does not apply to TDM SDSL/SHDSL cards.

   The **`Send Command:`** field is highlighted.

5. Type **yes** at the **`yes/no:`** prompt to execute the reset.

NOTE:

If a DSL card has been reset, but still does not appear on the screen, its configuration may have been corrupted. Reset the card again. This time, however, answer **yes** at the **`Clear NVRAM`** prompt. If the card then appears on the screen, it must be reconfigured. If the card does not appear on the screen, it may need to be replaced.

Configuring the IDSL Clock

Use the IDSL Clock Configuration screen to configure the IDSL clock source for each 8303/8304 IDSL card in the chassis.

▶ Procedure

To configure an IDSL slot:

1. Follow this menu sequence:

   Configuration → *Slot* → *IDSL Clock Setup* (**A-G-B**)

   The IDSL Clock Configuration screen appears.

2. Type the slot number of the DSL card at the **`Clock Config Card/Slot <nn or DSLnn>`** prompt.

3. Enter one of the following for NET_CLOCK1 and NET_CLOCK2:

   — **0**: Tristate. IDSL port clocks will use the local DSP clock for timing. The backplane I/O is tristated. This selection is not recommended.

   — **1**: Synchronize to the System Clock. IDSL port clocks will synchronize to the system clock (from the backplane). All IDSL port cards except one should be configured to this setting.

   — **3**: Drive System Clock. The system clock will be driven (output) from the card in this slot to the backplane. The card in this slot has one port configured to NT and is connected to an external clock source. Only one IDSL port card can be selected to drive the system clock.

4. Press Enter and the **`Save Changes? (Yes/No):`** prompt appears. Enter your desired response.

NOTE:

Because of these timing features, an 8820 or 8610 GranDSLAM with an MCP card is required when there is an IDSL card in the chassis.

Slot (DSL Cards) Menu Options

To access the DSL Cards menu, follow this menu selection sequence:

MCC Main Menu → *Configuration* → *Slot* (**A-G**)

Table 4-8. Slot (DSL Cards) Menu Options (1 of 2)

Reset Slot (Reset DSL Slot)	**A-G-A**
Allows you to reset a DSL card in any slot. The reset should be performed if there is a card in a slot that does not appear on the card selection screen. After entering the card number, selecting the command that will be sent (ForceBootP or reset), and confirming the reset, the MCC sends a reset signal via the backplane to the selected card. This screen allows you to ForceBootP (a nondisruptive reset), Reset (a minor disruption of less than 30 seconds), or Clear NVRAM (reset card and restore factory defaults). **DSL Card/Slot #** – Virtual (as opposed to physical) slot number of the DSL card. In the 8610 DSLAM, Slot #1 contains the MCC card and appears as virtual Slot# 19. Physical Slot #2 and #3 appear as Slots #1 and #2. **Command** – ForceBootP/Reset. ForceBootP will only work for cards with T1 and E1 connections. **Clear NVRAM also** – Yes/No. **Send Command** – Yes/No. NOTE: If you select yes (in the **`Clear NVRAM`** prompt), you permanently remove most of the configuration information you have stored on this card and all IP addresses and routing tables will need to be reentered. The system will perform a reset and return to the factory settings. This function does not apply to TDM SDSL/SHDSL cards. If a DSL card has been reset, but still does not appear on the screen, its configuration may have been corrupted and the card should be reset again. This time answer yes at the **`Clear NVRAM`** prompt. If the card appears on the screen, it needs to be reconfigured. If the card does not appear on the screen, it may need to be replaced. Contact your sales representative.	

Table 4-8. Slot (DSL Cards) Menu Options (2 of 2)

IDSL Clock Setup (IDSL Clock Configuration)	A-G-B

Allows you to configure the IDSL system clock distribution for the chassis. There are two available clock circuits in the backplane (NET_CLOCK1 and NET_CLOCK2). You can configure each source independently, but only one circuit (NET_CLOCK1, if not already assigned to another port card type) needs to be used for the IDSL system clock.

NOTES:

The following rules apply to the 8810/8820 chassis:

- More than one card cannot drive NET_CLOCK1
- More than one card cannot drive NET_CLOCK2
- No card can derive both NET_CLOCKs

The following rules apply to the 8610 chassis when stacked and connected together:

- More than one card cannot drive NET_CLOCK1 and more than one card cannot drive NET_CLOCK2 applies for each individual chassis. Therefore, slot numbers (2,3), (4–6), (7–9), (10–12), (13–15), and (15–18) must satisfy the conditions separately.
- No card can derive both NET_CLOCKs

DSL Card/Slot # – Virtual (as opposed to physical) slot number of the DSL card. In the 8610 DSLAM, Slot #1 contains the MCC card and appears as virtual Slot# 19. Physical Slot #2 and #3 appear as Slots #1 and #2.

Clock Configuration for NET_CLOCK1/NET_CLOCK2 – 0/1/3 (Default = 1). Configure each clock circuit for one of the following:

- 0: Tristate. IDSL card will use local DSP card for timing.
- 1: Synchronize to System Clock. The IDSL port card in this slot will synchronize to the system clock from the chassis backplane.
- 3: Drive System Clock. The system clock will be driven (output) from the card in this slot to the chassis backplane. The card in this slot must have one port configured to NT and will be connected to an external clock source. Only one IDSL card can be selected to drive the system clock.

SYSLOG Menu

The SYSLOG selection causes the SYSLOG screen to appear. See Table 4-9, SYSLOG Option. To access the Syslog selection, follow this menu selection sequence:

MCC Main Menu → *Configuration* → *Syslog* (**A-H**)

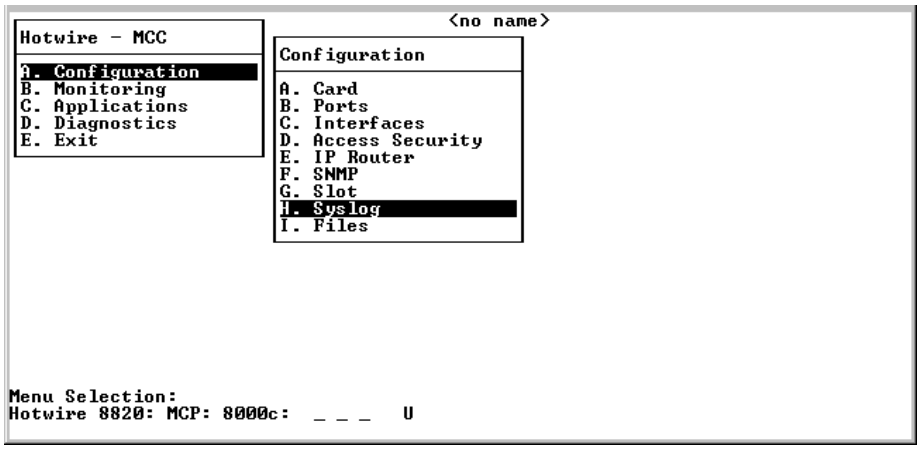


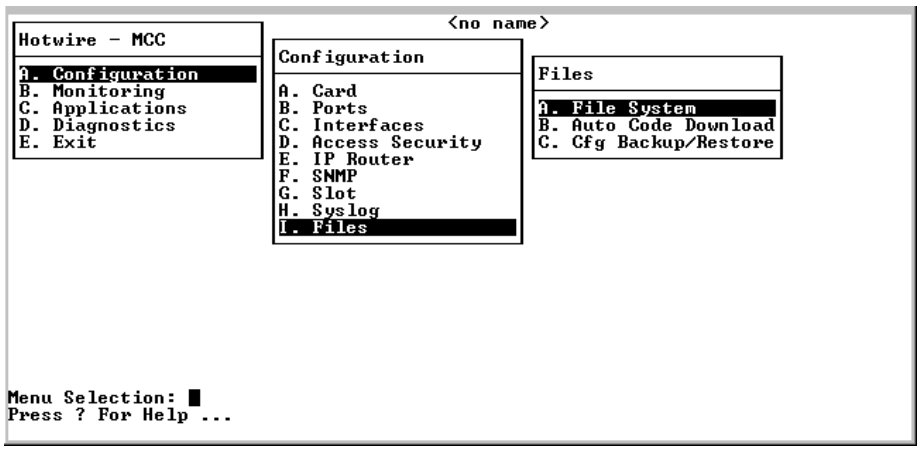
Table 4-9. SYSLOG Option

Syslog	**A-H**
Allows you to customize SYSLOG messages. **FTP Server File Transfer Statistics** – Enable/Disable (Default = disable). When enabled, the FTP server detail of any file transfer will be recorded in the SYSLOG. **TFTP Server File Transfer Statistics** – Enable/Disable (Default = disable). When enabled, the TFTP server detail of any file transfer will be recorded in the SYSLOG.	

Files Menu

To access the Files menu, follow this menu selection sequence:

MCC Main Menu → *Configuration* → *Files* (**A-I**)



The Files menu provides the following selections:

- **A. File System** – Changes directories, lists files/directories, and renames/deletes files in the MCC card's Flash File System (FFS).
- **B. Auto Code Download** – Automatically downloads firmware files from the FFS to cards in the DSLAM.
- **C. Cfg Backup/Restore** – Automatically backs up the card configuration and resynchronizes the backup files.

See Table 4-10, Files Menu Options, for information about options available from the Files menu.

Configuring Automatic Backup of Card Configuration and Resynchronization of Backup Files

Use the Configuration Backup/Restoral screen to schedule automatic backup of card configuration and to resynchronize the backup files.

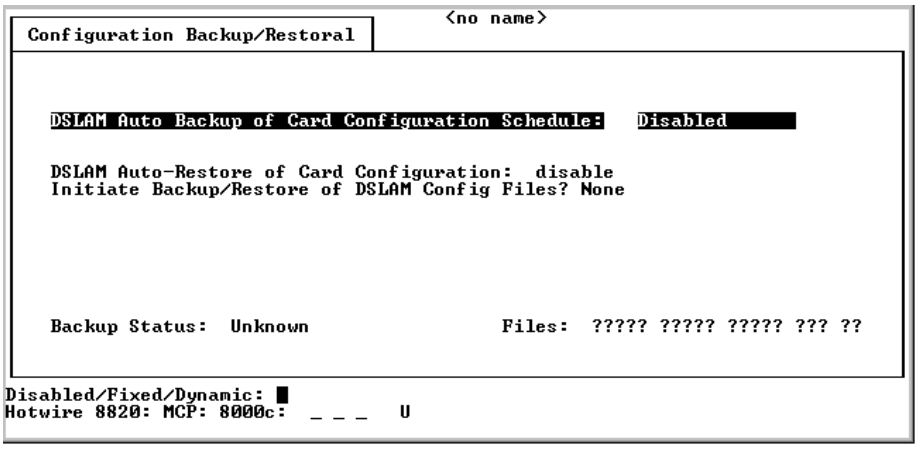
▶ Procedure

To configure automatic backup of the card configuration:

1. Follow this menu sequence:

   Configuration → *Files* → *Cfg Backup/Restore* (**A-I-C**)

   The Configuration Backup/Restoral screen appears.


<no name>
Configuration Backup/Restoral
DSLAM Auto Backup of Card Configuration Schedule: Disabled
DSLAM Auto-Restore of Card Configuration: disable
Initiate Backup/Restore of DSLAM Config Files? None
Backup Status: Unknown
Files: ????? ????? ????? ??? ??
Disabled/Fixed/Dynamic:
Hotwire 8820: MCP: 8000c: _ _ _ U

2. Set up or disable the Automatic Configuration Backup feature. This feature allows you to automatically back up the configuration files of the MCC, SCM and port cards onto the Flash File System (FFS). When enabled, auto backup uploads the configuration of each device onto the FFS according to the schedule selected.

   NOTE:

   This feature does not apply to any Model 8335/8365 card with a firmware version below GranDSLAM 2.0, nor to any other port card with a firmware version below GranDSLAM 2.1.

In the DSLAM Auto Backup of Card Configuration Schedule field, select one of the following options for automatic configuration backup:

Select . . .	To . . .
Disable	Disable the auto configuration backup feature.
Fixed	Automatically back up files at the selected day and time (default = 9 PM daily), where day is Daily, or Mon, Tues, Wed, Thurs, Fri, or Sat; time is hour (1–12), minute (0–59), AM/PM.
Dynamic	Automatically back up files in the selected amount of time since the last configuration change, where time is entered in the format hh:mm (hh = 0–24 hours, mm = 0–59 minutes). This is the default. The default dynamic schedule is 30 minutes.

3. In the DSLAM Auto Restore of Card Configuration field, enter **Enable** to restore a card configuration when a change in serial number is detected.
4. In the Initiate Backup/Restore of DSLAM Config Files field, enter **Backup** (back up configuration files to the MCC card's FFS), **Restore** (restore configuration files from the MCC card's FFS) or **None**. Once a backup or restore of the files is requested, it must finish before another backup or restoral can be started.
5. Press Ctrl-z to save the changes and return to the Card menu.

Table 4-10. Files Menu Options (1 of 2)

File System	A-I-A

Allows you to change directories, list files/directories, and rename/delete files in the flash file system. Up to 32 characters are allowed for file and directory names. The full path name length is limited to 40 characters. File names are case-sensitive. Supported commands are listed in the online Help.

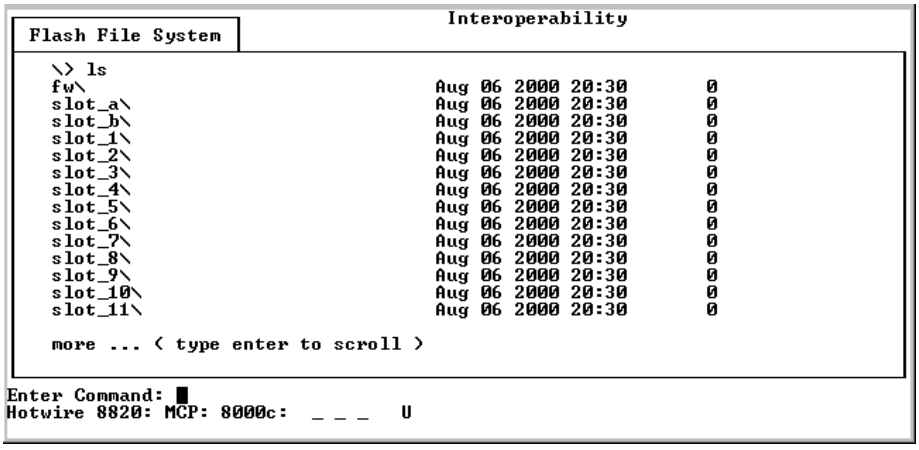
Type **ls** to display the directories. The information displayed in the flash file system includes the directory name, file name, file size, file date, product model and firmware version, free flash space, and memory space used by the files in the current directory.

The firmware directory (fw) contains the code image software for downloading port cards. Multiple code files can be stored here (one for each card model in the DSLAM). You can upgrade the firmware in the in the port cards by downloading the firmware stored in this file system directly from the MCP card.

Port card configurations are stored in the configuration directories (such as slot_1). Only one file can be stored in each of these directories.

A Flash File System screen is shown below.

See Appendix A, *Upgrade Procedures*, to FTP a firmware file to the MCC card's FFS.


Interoperability
Flash File System
\> ls
fw\ Aug 06 2000 20:30 0
slot_a\ Aug 06 2000 20:30 0
slot_b\ Aug 06 2000 20:30 0
slot_1\ Aug 06 2000 20:30 0
slot_2\ Aug 06 2000 20:30 0
slot_3\ Aug 06 2000 20:30 0
slot_4\ Aug 06 2000 20:30 0
slot_5\ Aug 06 2000 20:30 0
slot_6\ Aug 06 2000 20:30 0
slot_7\ Aug 06 2000 20:30 0
slot_8\ Aug 06 2000 20:30 0
slot_9\ Aug 06 2000 20:30 0
slot_10\ Aug 06 2000 20:30 0
slot_11\ Aug 06 2000 20:30 0
more ... (type enter to scroll)
Enter Command:
Hotwire 8820: MCP: 8000c: _ _ _ U

Auto Code Download	A-I-B

Allows you to automatically download firmware files stored in the MCC card's FFS to cards in the DSLAM. If more than one image exists in the FFS directory, the latest firmware release image is chosen for downloading to the port card. After an auto code download has been completed or attempted, it is reported to the syslog (**B-A-C**).

DSLAM Auto Download of Firmware Files – Enable/Disable (Default = disable). When enabled, firmware stored in the MCC card's FFS will be automatically downloaded. Upon power-up, each card will determine whether a download is required and initiate the download if determined necessary.

NOTES:

- Port cards must have version GranDSLAM 2.0 or greater firmware to allow auto download of firmware files.
- OpenLane SLM version 5.5 or greater must be installed.
- Evaluate all files in the FFS to ensure that no incorrect firmware files are present.
- SN firmware is not automatically upgraded. Communication with the SN may be lost if upgrading the port card results in incompatible firmware levels. If this occurs, it may be necessary to return the port card to an older firmware version, upgrade the SN, then return the port card firmware to the newer version.

Table 4-10. Files Menu Options (2 of 2)

Cfg Backup/Restore	A-I-C

DSLAM Auto Backup of Card Configuration Schedule – Enter one of the following:

- **Disable** to disable auto configuration backup.
- **Fixed** to automatically back up files on a selected day and time, where day is Daily, or Mon, Tues, Wed, Thurs, Fri, or Sat; time is hour (1–12), minute (0–59), AM/PM.
- **Dynamic** to automatically back up files in the selected amount of time after a configuration change, where hh=0–24 hours, mm=0–59 minutes. This is the default.

Fixed Schedule – Enter time in the format d on hh:mm AM/PM, where day (d) is Daily, or Mon, Tues, Wed, Thurs, Fri, or Sat; time is hour (1–12), minute (0–59), AM/PM. This field only appears if Fixed is selected for DSLAM Auto Backup of Card Configuration Schedule.

Dynamic Schedule – Enter time in the format hh:mm, where hh=0–24 hours, mm=0–59 minutes (Default = 30 minutes). This field only appears if Dynamic is selected for DSLAM Auto Backup of Card Configuration Schedule.

DSLAM Auto Restore of Card Configuration – Enable/Disable. When enabled, a card configuration is restored when a new card of the same type is installed (as determined by a check of the card's serial number), or when the manual reset feature is selected. If the configuration is not compatible because the port cards are of different types, then the configuration is not downloaded.

Initiate Backup/Restore of DSLAM Config Files? – Backup/Restore/None (Default = None). Enter whether to back up configuration files to the MCC card's FFS, restore configuration files from the MCC card's FFS, or neither.

Backup Status – (Read-only) For manual backups, displays the current status of the file backup (Unknown, In Progress, Success, or Failure).

Files – (Read-only) For manual backups, displays the status of the configuration backup for each slot in the DSLAM:

- **?** = unknown (status unavailable)
- **r** = reloaded (backup successful)
- **-** = pending backup
- **x** = empty slot
- **F** = Failure (could not back up configuration file)

Monitoring Menu Options

5

Overview

This chapter describes the options on the Monitoring menu of the MCC card. The Hotwire DSL system lets you monitor all cards in the chassis. You monitor DSL and MCC card operations by selecting various options from the Monitoring menu. To access the Monitoring menu, follow this menu selection sequence:

MCC Main Menu → Monitoring

The Monitoring menu selections are described in the following sections:

- *Card Status Menu Options* on page 5-2
- *Physical Layer Menu Options* on page 5-6
- *Interfaces Menu Options* on page 5-10
- *Network Protocol Menu Options* on page 5-13
- *IP Router Menu Options* on page 5-25
- *Servers Menu Options* on page 5-30
- *Files Menu Options* on page 5-32

This chapter presents information on how to access these menus and their submenus to monitor card status and performance statistics.

NOTE:

Most Monitoring menus are read-only. The information helps you gather pertinent data and isolate potential problems.

— For diagnostic tools, see *Chapter 7, Diagnostics Menu Options.*

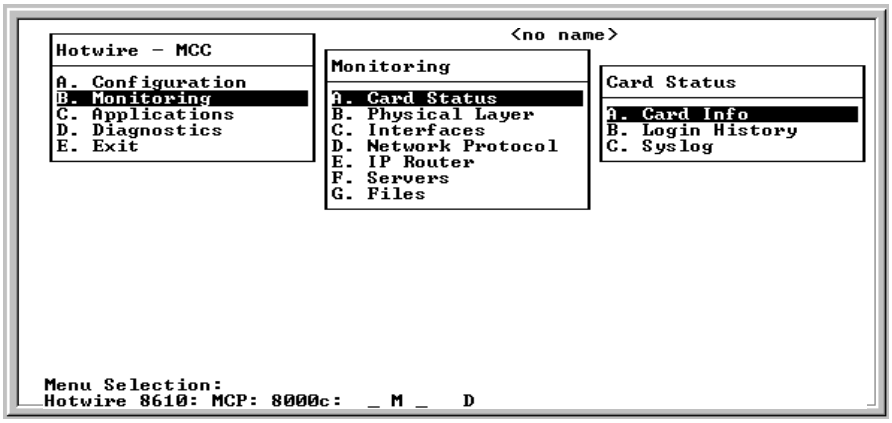
— For troubleshooting DSL system problems, see Chapter 8, *Troubleshooting*.

— For information about monitoring and troubleshooting specific DSL Cards, see the *Hotwire MVL, ReachDSL, RADSL, IDSL, and SDSL Cards, Models 8310, 8312/8314, 8510/8373/8374, 8303/8304, and 8343/8344, User's Guide*.

Card Status Menu Options

To access the Card Status menu, follow this menu selection sequence:

MCC Main Menu → *Monitoring* → *Card Status* (**B-A**)



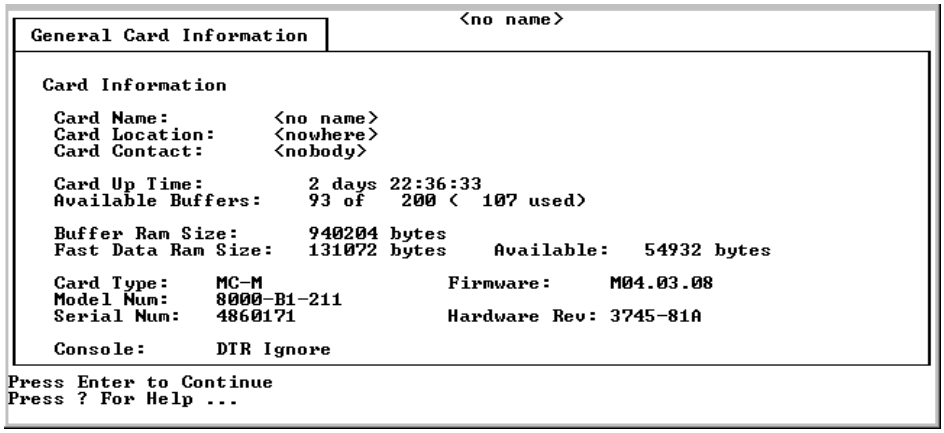
- **A. Card Info** – General card information such as card type, model and serial number, firmware, and hardware version number.
- **B. Login History** – The 10 most recent logins.
- **C. Syslog** – A sequential timestamp list of system operational-type errors, such as alarms, cards added/removed from chassis and invalid IP addresses.

Displaying General Card Information

To display general card information, follow this menu selection sequence:

Monitoring → *CardStatus* → *Card Info* (**B-A-A**)

The General Card Information screen appears.


<no name>
General Card Information
Card Information
Card Name: <no name>
Card Location: <nowhere>
Card Contact: <nobody>
Card Up Time: 2 days 22:36:33
Available Buffers: 93 of 200 (107 used)
Buffer Ram Size: 940204 bytes
Fast Data Ram Size: 131072 bytes Available: 54932 bytes
Card Type: MC-M Firmware: M04.03.08
Model Num: 8000-B1-211
Serial Num: 4860171 Hardware Rev: 3745-81A
Console: DTR Ignore
Press Enter to Continue
Press ? For Help ...

The General Card Information screen displays the information listed in Table 5-1, General Card Information Screen.

Table 5-1. General Card Information Screen

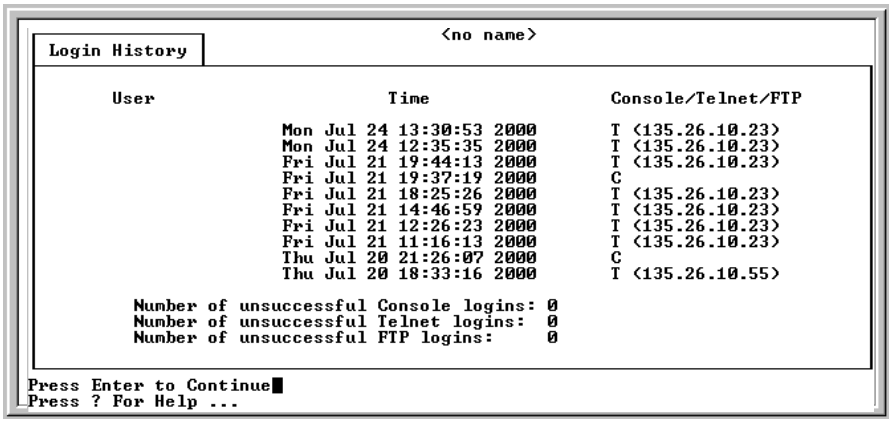
General Card Information	B-A-A
Card Name – Name assigned to the card.	
Card Location – Physical location of the system.	
Card Contact – Name or number of the person responsible for the card.	
Card Up Time – Length of time the system has been running.	
Available Buffers – Number of buffers not in use.	
Buffer Ram Size – Size of the Buffer Ram.	
Fast Data Ram Size – Total Fast Data Ram.	
Available – Available Fast Data Ram.	
Card Type – Type of card.	
Model Num – Model number of card.	
Serial Num – Serial number of card.	
Firmware – Version of firmware.	
Hardware Rev – Version of hardware.	
Console – The field says either DTR (Data Terminal Ready) Ignore or DTR aware. DTR Ignore means that you have an older version of modem connection hardware. If you primarily use a direct terminal connection, this may not be a problem. If you primarily use a modem to connect to the system, call your sales or service representative for hardware information.	

Displaying Login History

To display information about the 10 most recent logins, follow this menu selection sequence:

Monitoring → *CardStatus* → *Login History* (**B-A-B**)

The Login History screen appears.


<no name>
Login History
User
Time
Console/Telnet/FTP
Mon Jul 24 13:30:53 2000 T (135.26.10.23)
Mon Jul 24 12:35:35 2000 T (135.26.10.23)
Fri Jul 21 19:44:13 2000 T (135.26.10.23)
Fri Jul 21 19:37:19 2000 C
Fri Jul 21 18:25:26 2000 T (135.26.10.23)
Fri Jul 21 14:46:59 2000 T (135.26.10.23)
Fri Jul 21 12:26:23 2000 T (135.26.10.23)
Fri Jul 21 11:16:13 2000 T (135.26.10.23)
Thu Jul 20 21:26:07 2000 C
Thu Jul 20 18:33:16 2000 T (135.26.10.55)
Number of unsuccessful Console logins: 0
Number of unsuccessful Telnet logins: 0
Number of unsuccessful FTP logins: 0
Press Enter to Continue
Press ? For Help ...

The Login History screen displays the information listed in Table 5-2, Login History Screen.

Table 5-2. Login History Screen

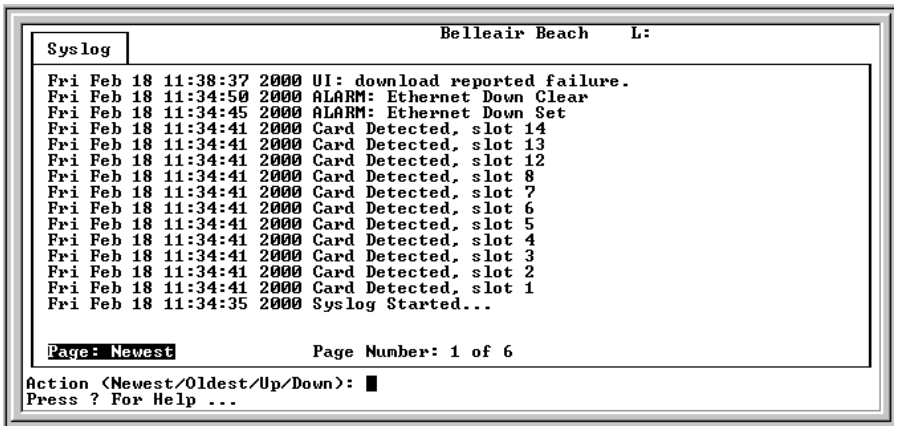
Login History	B-A-B
User – User ID.	
Time – Time of login.	
Console/Telnet/FTP – C (Console), T (Telnet), or F (FTP). Type of login and IP address of remote host.	
Number of unsuccessful Console logins – Number of incorrect console logins.	
Number of unsuccessful Telnet logins – Number of incorrect Telnet logins.	
Number of unsuccessful FTP logins – Number of incorrect FTP logins.	

Displaying System Errors

To display system errors, follow this menu selection sequence:

Monitoring → *CardStatus* → *Syslog* (**B-A-C**)

The Syslog screen appears.


Belleair Beach L:
Syslog
Fri Feb 18 11:38:37 2000 UI: download reported failure.
Fri Feb 18 11:34:50 2000 ALARM: Ethernet Down Clear
Fri Feb 18 11:34:45 2000 ALARM: Ethernet Down Set
Fri Feb 18 11:34:41 2000 Card Detected, slot 14
Fri Feb 18 11:34:41 2000 Card Detected, slot 13
Fri Feb 18 11:34:41 2000 Card Detected, slot 12
Fri Feb 18 11:34:41 2000 Card Detected, slot 8
Fri Feb 18 11:34:41 2000 Card Detected, slot 7
Fri Feb 18 11:34:41 2000 Card Detected, slot 6
Fri Feb 18 11:34:41 2000 Card Detected, slot 5
Fri Feb 18 11:34:41 2000 Card Detected, slot 4
Fri Feb 18 11:34:41 2000 Card Detected, slot 3
Fri Feb 18 11:34:41 2000 Card Detected, slot 2
Fri Feb 18 11:34:41 2000 Card Detected, slot 1
Fri Feb 18 11:34:35 2000 Syslog Started...
Page: Newest
Page Number: 1 of 6
Action (Newest/Oldest/Up/Down):
Press ? For Help ...

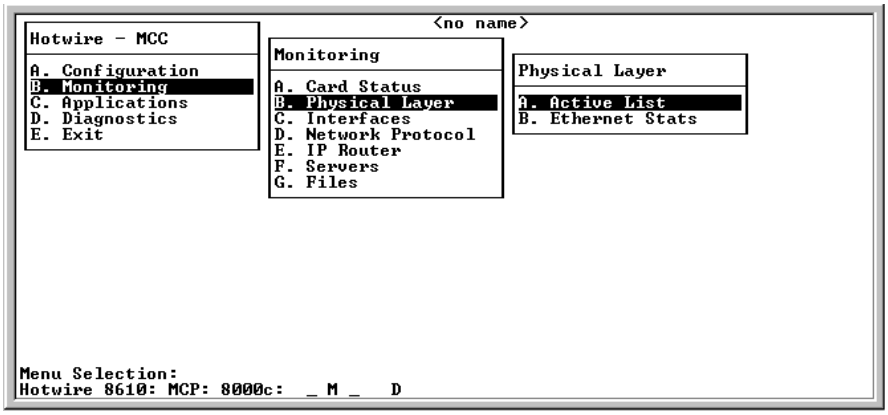
The Syslog screen displays a sequential timestamp list of operational errors (such as invalid IP addresses) by date and error. There is one logged error per line in a downward scrolling list.

Physical Layer Menu Options

The Physical Layer menu options allow you to display read-only system information about physical ports.

To access the Physical Layer menu, follow this menu selection sequence:

MCC Main Menu → *Monitoring* → *Physical Layer* (**B-B**)



The Physical Layer menu provides the following options:

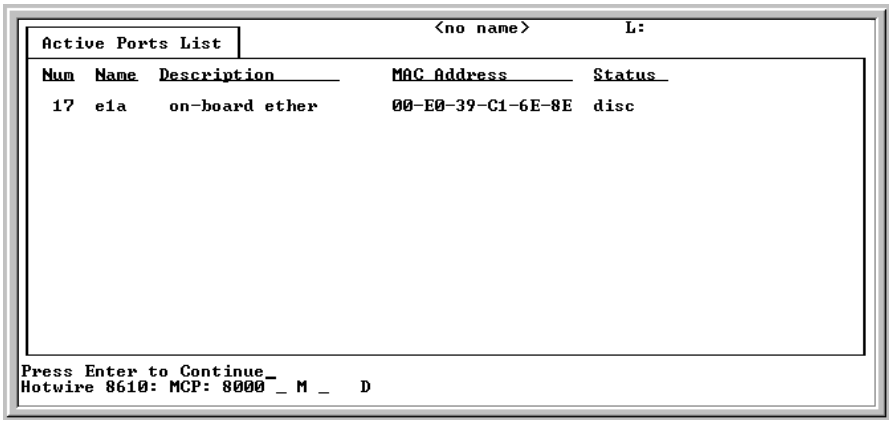
- **A. Active List** – Displays the status of all active ports.
- **B. Ethernet Stats** – Displays Ethernet statistics on the LAN port (e1a).

Displaying Active Ports

To display the status of all active ports, follow this menu selection sequence:

Monitoring → *Physical Layer* → *Active List* (**B-B-A**)

The Active Ports List screen appears.


Active Ports List
<no name>
L:
Num Name Description MAC Address Status
17 e1a on-board ether 00-E0-39-C1-6E-8E disc
Press Enter to Continue_
Hotwire 8610: MCP: 8000 _ M _ D

The Active Ports List screen displays the information listed in Table 5-3, Active Ports List Screen.

Table 5-3. Active Ports List Screen

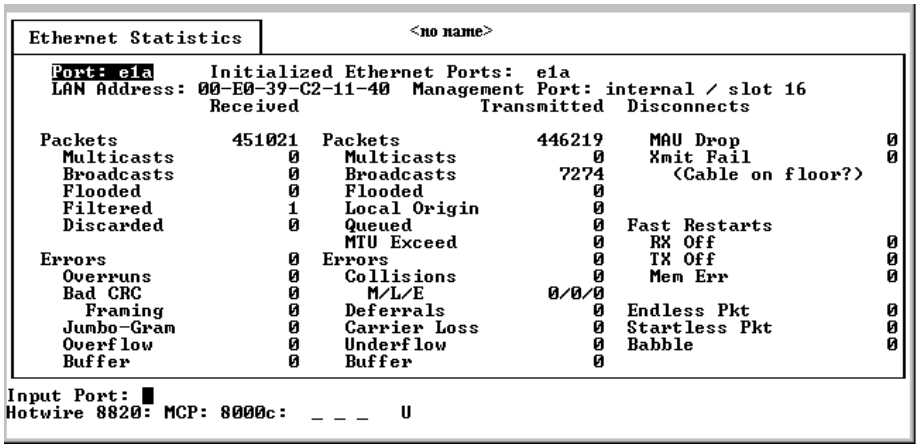
Active Ports List	B-B-A
Num – Number of the port. **Name** – Name of the port. **Description** – Type of port (for example, Ethernet). **MAC Address** – MAC address of the active port. (Internal dummy address is used for non-Ethernet ports.) **Status** – In-use or disconnected.	

Displaying Ethernet Statistics

To display statistics of the LAN port (e1a), follow this menu selection sequence:

Monitoring → *Physical Layer* → *Ethernet Stats* (**B-B-B**)

The Ethernet Statistics screen appears.



NOTE:

You may press Ctrl-r at any time to reset the counters.

The Ethernet Statistics screen displays the information listed in Table 5-4, Ethernet Statistics Screen.

Table 5-4. Ethernet Statistics Screen

Ethernet Statistics	B-B-B

Port – Name of port (e1a).

Initialized Ethernet Ports – e1a (there is only one Ethernet port on the MCC card).

LAN Address – LAN (or MAC) address of the Ethernet port.

Management Port – The type of management port (internal/external) and the slot number of the management port.

Bytes Received – Number of bytes received by the Ethernet port (i.e., a running account of how many bytes have been received since the last reset).

Packets Received – Running account of packets received by the Ethernet port since the last reset and what type:

- Multicasts – Single packets copied to a specific subset of network addresses.
- Broadcasts – Messages sent to all network destinations.
- Flooded – Information received, then sent out to each of the interfaces.
- Filtered – Processes or devices that screen incoming information.
- Discarded – Packets discarded.

Errors Received – Number of errors received by the Ethernet port and what type:

- Overruns – No buffer space.
- Bad CRC – Cyclic Redundancy Check.
- Framing – Receiver improperly interprets set of bits within frame.
- Jumbo gram – Ethernet packet too long.
- Overflow – Part of traffic that is not carried.
- Buffer – No buffer space.

Bytes Transmitted – Number of bytes transmitted by the Ethernet port.

Packets Transmitted – Number of packets transmitted by the Ethernet port and what type (Multicasts, Broadcasts, Flooded, Local Origin, Queued, MTU Exceeded).

Errors Transmitted – Number and type of errors transmitted by the Ethernet port and what type:

- Collisions:
  - M = Multi-collision frames – not counted this release and always set to 0.
  - L = Late collisions – collision detected often; at least 64 bytes have been transmitted.
  - E = Excessive collisions – port tried to send a packet 15 times without success.
- Deferrals
- Carrier Loss
- Underflow
- Buffer

Disconnects – Number of disconnects on the Ethernet port and what type:

- Disable – Transmit error, timed out.
- MAU drop – Transceivers dropped.
- Xmit fail – Transmit fail.

Fast Restarts – Number of fast restarts and what type (RX Off, TX Off, Mem Err).

Endless Pkt – Number of endless packets received on the Ethernet port.

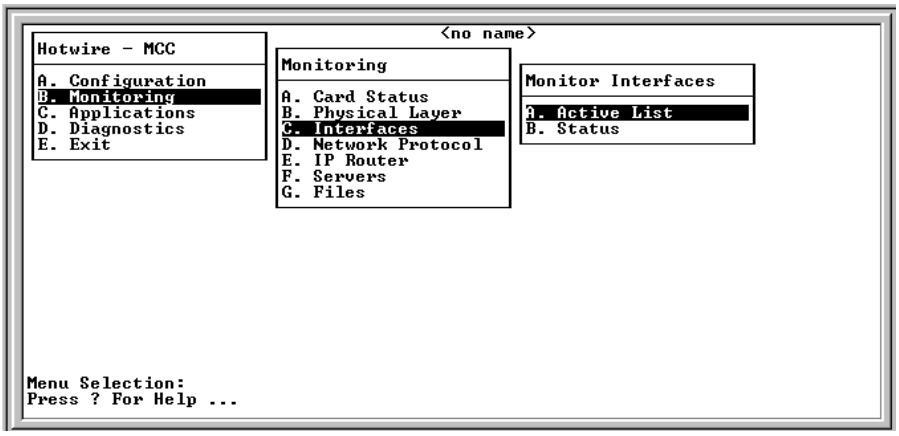
Startless Pkt – Number of startless packets received on the Ethernet port.

Babble – Number of garbled packets received due to crosstalk.

Interfaces Menu Options

To access the Interfaces menu, follow this menu selection sequence:

MCC Main Menu → *Monitoring* → *Interfaces* (**B-C**)



The Interfaces menu provides the following options:

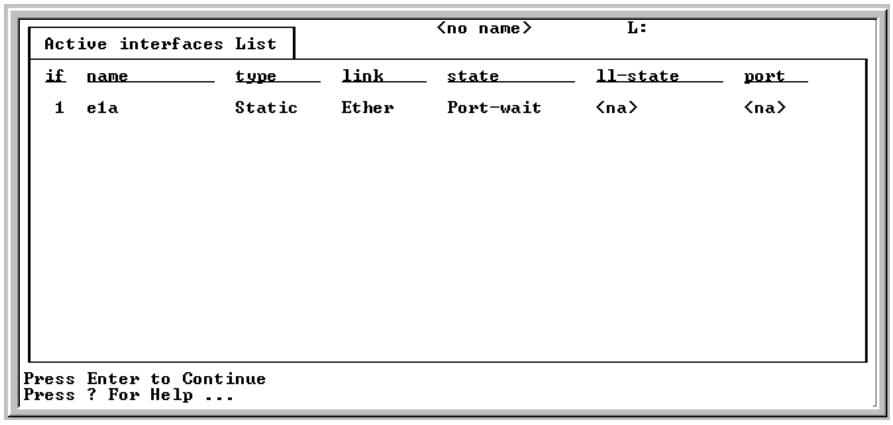
- **A. Active List** – Status of all active interfaces on the card.
- **B. Status** – Additional interface status information such as interface name, protocol, port, user name, interface type, and interface state.

Displaying Active Interfaces

To display the status of all active interfaces, follow this menu selection sequence:

Monitoring → *Interfaces* → *Active List* (**B-C-A**)

The Active Interfaces List screen appears.


Active interfaces List
<no name>
L:
if name type link state ll-state port
1 e1a Static Ether Port-wait <na> <na>
Press Enter to Continue
Press ? For Help ...

The Active Interfaces List screen displays the information listed in Table 5-5, Active Interfaces List Screen.

Table 5-5. Active Interfaces List Screen

Active Interfaces List	B-C-A
if – Number of the interface.	
name – Name of the interface.	
type – Interface type (static).	
link – Name of the protocol on the interface.	
state – Current state of the interface.	
ll-state – Not applicable.	
port – Port linked to this interface.	

NOTE:

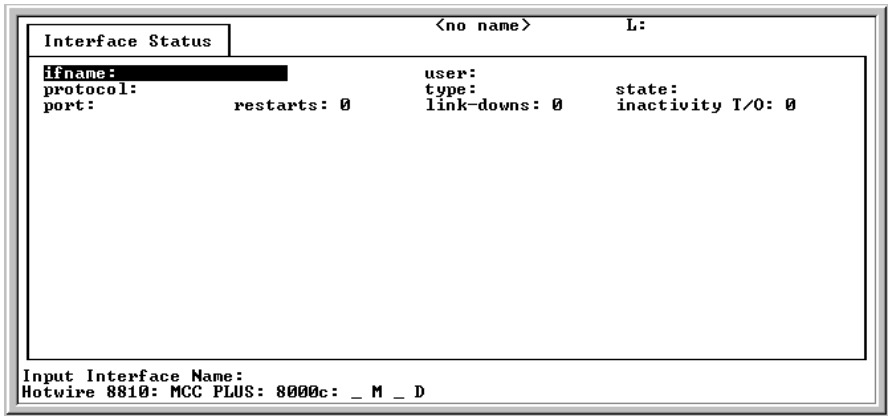
The only information that changes on the Active Interfaces List screen is the state (active or port-wait) column.

Displaying Additional Interface Status

To display additional interface information, follow this menu selection sequence:

Monitoring → *Interfaces* → *Status* (**B-C-B**)

The Interface Status screen appears.



The Interface Status screen displays the information listed in Table 5-6, Interface Status Screen.

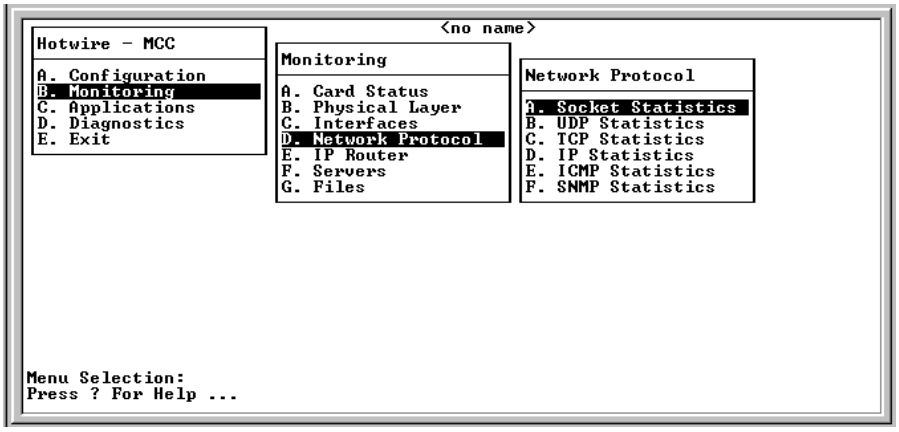
Table 5-6. Interface Status Screen

Interface Status	**B-C-B**
ifname – Enter the name of the desired interface (e1a).	
protocol – Type of protocol for the entered interface name.	
port – Port linked to this interface.	
restarts – Number of times the interface has been restarted.	
user – NA or none.	
type – Static.	
link-downs – Number of times the link has gone down.	
state – Active or prtwait (port-wait).	
inactivity T/O – Number of times the interface has timed out.	

Network Protocol Menu Options

To access the Network Protocol menu, follow this menu selection sequence:

MCC Main Menu → *Monitoring* → *Network Protocol* (**B-D**)



The Network Protocol menu provides the following options:

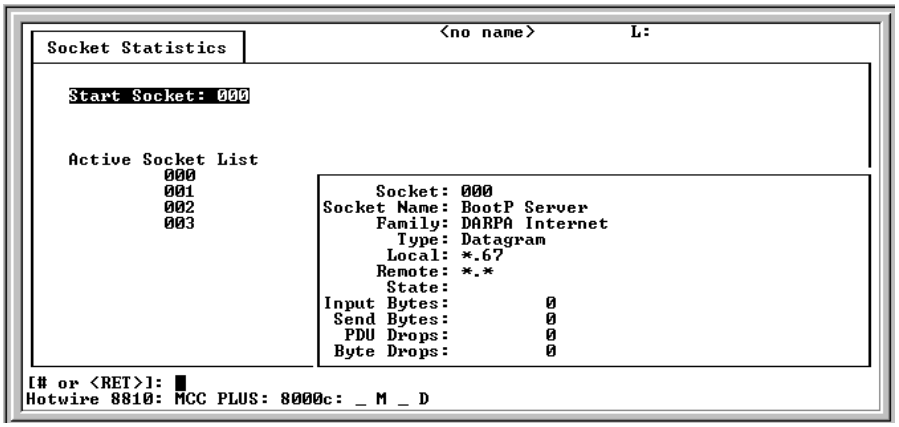
- **A. Socket Statistics** – Information about active sockets, such as socket name, socket type, input bytes and output bytes, and PDU and byte drops.
- **B. UDP Statistics** – UDP statistics, such as input packets, output packets, packets with checksum errors, and bad length packets.
- **C. TCP Statistics** – Summary of TCP activity (packets and bytes transmitted and received) and TCP connection activity on all interfaces on the card.
- **D. IP Statistics** – Summary of the IP activity on all interfaces on the card.
- **E. ICMP Statistics** – Summary of ICMP activity on all interfaces of the card.
- **F. SNMP Statistics** – SNMP statistics, such as number of get requests, number of set requests, and parsing errors.

Displaying Socket Statistics

To display information about active sockets, follow this menu selection sequence:

Monitoring → *Network Protocol* → *Socket Statistics* (**B-D-A**)

The Socket Statistics screen appears.



▶ Procedure

On this screen:

1. Type a valid socket number (from the Active Socket List) at the **`[# or <RET>]:`** prompt.
2. Press Enter.

The boxed, lower right area of the screen displays information and statistics about the application program assigned to the socket number you entered.

The Socket Statistics screen displays the information listed in Table 5-7, Socket Statistics Screen.

Table 5-7. Socket Statistics Screen

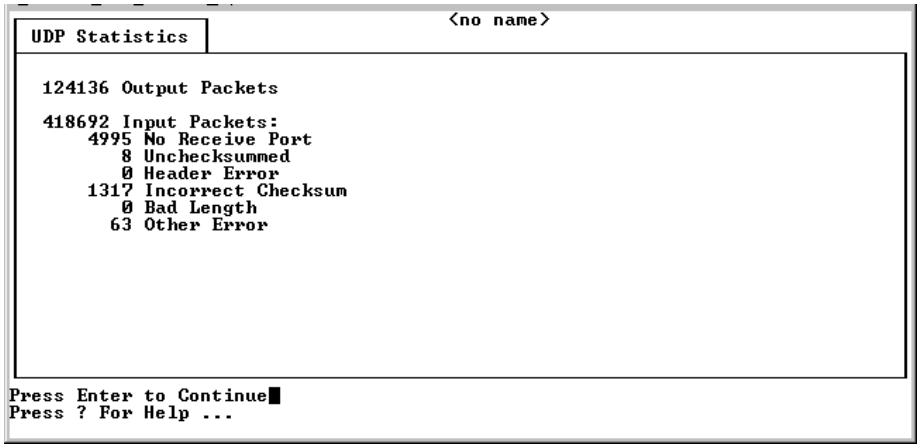
Socket Statistics	B-D-A
Start Socket – Enter the socket number to start the active socket list.	
Active Socket List – Lists the active sockets in the system.	
In addition, the lower right-hand corner of the screen displays a Socket Statistics window with detailed information about the selected socket.	
Socket – Socket number.	
Socket Name – Internal name of the socket.	
Family – Family of this socket (DARPA Internet).	
Type – Socket type (stream or datagram).	
Local – Port number on this card.	
Remote – Port number on remote card.	
State – Current state of the socket.	
Input Bytes – Bytes waiting in the socket for the owning application to process (will go to 0 when processed by the application).	
Send Bytes – Bytes waiting to be sent out to the remote machine.	
PDU Drops – Incoming packets dropped (usually due to a lack of space).	
Byte Drops – Outgoing packets dropped (usually due to a lack of space).	

Displaying UDP Statistics

To display information on UDP statistics, follow this menu selection sequence:

Monitoring → *Network Protocol* → *UDP Statistics* (**B-D-B**)

The UDP Statistics screen appears.



NOTE:

The counters increment in real time. You may press Ctrl-r at any time to reset them.

The UDP Statistics screen displays the information listed in Table 5-8, UDP Statistics Screen.

Table 5-8. UDP Statistics Screen

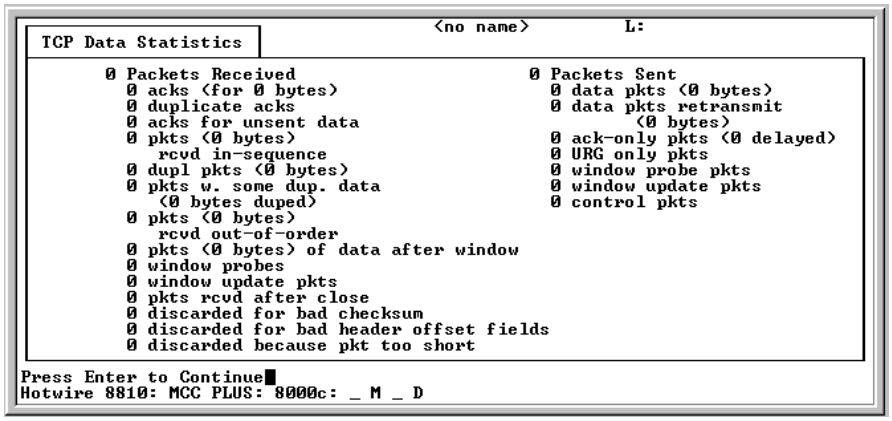
UDP Statistics B-D-B
Output Packets – UDP packets sent out of the card.
Input Packets – UDP packets coming into the card.
No Receive Port – UDP packets coming into the card that had no receive port waiting for this packet.
Unchecksummed – UDP packets coming into the card with no checksum.
Header Error – UDP packets coming into card that had an error with the packet header.
Incorrect Checksum – UDP packets coming into the card with a bad checksum.
Bad Length – Number of UDP packets coming into the card that are an illegal length (too short).
Other Error – Number of UDP packets coming into the card that had an error, but not one of the above.

Displaying TCP Statistics

To display a summary of TCP data activity, follow this menu selection sequence:

Monitoring → *Network Protocol* → *TCP Statistics* (**B-D-C**)

The TCP Data Statistics screen appears.


TCP Data Statistics
<no name>
L:
0 Packets Received
0 acks (for 0 bytes)
0 duplicate acks
0 acks for unsent data
0 pkts (0 bytes)
rcvd in-sequence
0 dupl pkts (0 bytes)
0 pkts w. some dup. data
(0 bytes duped)
0 pkts (0 bytes)
rcvd out-of-order
0 pkts (0 bytes) of data after window
0 window probes
0 window update pkts
0 pkts rcvd after close
0 discarded for bad checksum
0 discarded for bad header offset fields
0 discarded because pkt too short
0 Packets Sent
0 data pkts (0 bytes)
0 data pkts retransmit
(0 bytes)
0 ack-only pkts (0 delayed)
0 URG only pkts
0 window probe pkts
0 window update pkts
0 control pkts
Press Enter to Continue
Hotwire 8810: MCC PLUS: 8000c: _ M _ D

NOTES:

— The left column of the TCP Statistics screen displays information for received data and the right column displays information for transmitted data.

— The counters increment in real time. You may press Ctrl-r at any time to reset them.

The TCP Data Statistics screen displays the information listed in Table 5-9, TCP Data Statistics Screen.

Table 5-9. TCP Data Statistics Screen

TCP Data Statistics	B-D-C

Left column (received):

Packets Received – Number of TCP packets received by the card.

acks – Number of acknowledgements received for transmitted packets. (Also shows the number of bytes that were acknowledged as received by the remote system.)

duplicate acks – Number of duplicate acknowledgements (acks) received.

acks for unsent data – Number of acknowledgements received for data that has not been sent yet.

pkts (bytes) rcvd in-sequence – Number of packets/bytes correctly received in sequence for data that had to be split in multiple TCP packets.

dupl pkts (bytes) – Number of duplicate packets (bytes) received.

pkts (bytes) w. some dup. data – Number of packets (bytes) with some duplicated data. (Duplicated data is discarded by TCP.)

pkts (bytes) rcvd out-of-order – Packets (bytes) received out of order.

pkts (bytes) of data after window – Packets (bytes) of data received after our receive window is full.

window probes – Packets received looking for space in our receive window.

window update pkts – Packets received from the remote system advertising a new window size.

pkts rcvd after close – Packets received after the TCP connection is shut down.

discarded for bad checksum – Packets discarded because the checksum failed.

discarded for bad header offset fields – Packets discarded because the TCP header was corrupted.

discarded because pkt too short – Packets discarded because the packet was too short (not a complete TCP header).

Right column (transmitted):

Packets Sent – Number of TCP packets sent by the card.

data pkts (bytes) – Sent packets (bytes) that were data packets instead of TCP control packets.

data pkts retransmit – Number of packets/bytes that had to be transmitted.

ack-only pkts – Number of sent packets that contained only an acknowledgment of a received packet.

URG only pkts – Number of packets that contained only an Urgent flag and no data.

window probe pkts – Number of packets that were window probes.

window update pkts – Number of packets that were advertising our new window size.

control pkts – Number of control packets sent (SYN, FIN, or RST flag).

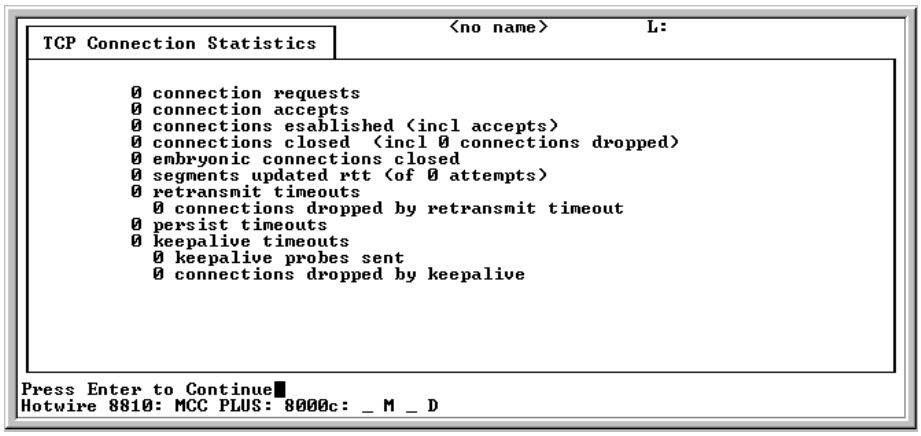
- SYN = synchronization packet (synchronization sequence number)
- FIN = finish packet (end of transmission)
- RST = reset packet (reset connection).

Displaying TCP Connection Statistics

To display a summary of the TCP connection activity on all interfaces on the card, follow this menu selection sequence:

Monitoring → *Network Protocol* → *TCP Statistics* (**B-D-C**)

After the TCP Data Statistics screen appears, press Enter to access the TCP Connection Statistics screen.


<no name> L:
TCP Connection Statistics
0 connection requests
0 connection accepts
0 connections esablished (incl accepts)
0 connections closed (incl 0 connections dropped)
0 embryonic connections closed
0 segments updated rtt (of 0 attempts)
0 retransmit timeouts
0 connections dropped by retransmit timeout
0 persist timeouts
0 keepalive timeouts
0 keepalive probes sent
0 connections dropped by keepalive
Press Enter to Continue
Hotwire 8810: MCC PLUS: 8000c: _ M _ D

The TCP Connection Statistics screen displays the information listed in Table 5-10, TCP Connection Statistics Screen.

Table 5-10. TCP Connection Statistics Screen

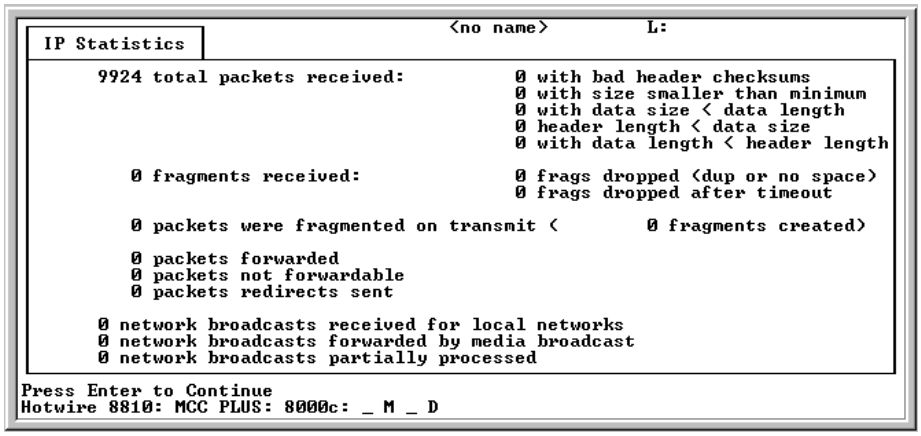
TCP Connection Statistics	B-D-C
connection requests – Number of TCP connections initiated by a process on this card.	
connection accepts – Number of TCP connections accepted by this card.	
connections established – Number of connections established.	
connections closed – Connections closed.	
embryonic connections closed – Connections dropped before data transfer.	
segments updated rtt – Number of packets that updated the Round Trip Time (RTT) and the total number of times TCP attempted to update the RTT.	
retransmit timeouts – Number of times a packet was transmitted because it was not acknowledged and the number of times a connection was dropped because a packet could not be transmitted.	
connections dropped by retransmit timeout – Number of connections dropped because the retransmit timer failed to get any responses.	
persist timeouts – Number of times the TCP persistence timer went off and sent a probe to the remote system.	
keepalive timeouts – Number of times a TCP keepalive request timed out.	
keepalive probes sent – Number of TCP keepalive probes sent.	
connections dropped by keepalive – Number of connections dropped because the keepalive timer failed to get any responses.	

Displaying IP Statistics

To display a summary of IP activity on all interfaces, follow this menu selection sequence:

Monitoring → *Network Protocol* → *IP Statistics* (**B-D-D**)

The IP Statistics screen appears.


(no name) L:
IP Statistics
9924 total packets received:
0 with bad header checksums
0 with size smaller than minimum
0 with data size < data length
0 header length < data size
0 with data length < header length
0 fragments received:
0 frags dropped (dup or no space)
0 frags dropped after timeout
0 packets were fragmented on transmit (0 fragments created)
0 packets forwarded
0 packets not forwardable
0 packets redirects sent
0 network broadcasts received for local networks
0 network broadcasts forwarded by media broadcast
0 network broadcasts partially processed
Press Enter to Continue
Hotwire 8810: MCC PLUS: 8000c: _ M _ D

The IP Statistics screen displays the information listed in Table 5-11, IP Statistics Screen.

Table 5-11. IP Statistics Screen

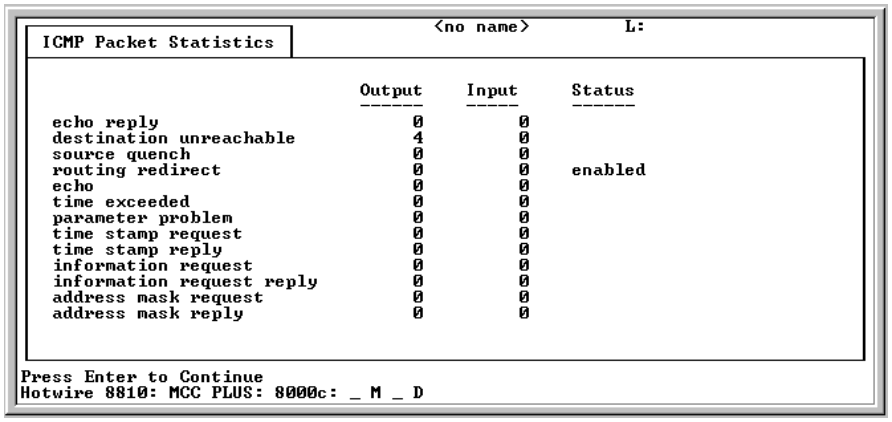
IP Statistics B-D-D
total packets received – Total number of IP packets received by this card, with errors (classified into five categories) on the right of the screen.
fragments received – Number of packet fragments received, with dropped fragments (classified into two categories) on the right of the screen.
packets were fragmented on transmit – Number of packets that were fragmented on transmit and the number of fragments that were created by those packets.
packets forwarded – Number of packets that were forwarded to another system.
packets not forwardable – Number of packets that could not be forwarded. (Usually due to packet errors or routing problems.)
packet redirects sent – Number of redirect messages sent to other systems because they incorrectly sent a packet to this card.
network broadcasts received for local networks – Number of network broadcasts received for local networks.
network broadcasts forwarded by media broadcast – Number of network broadcasts for local networks sent.
network broadcasts partially processed – Number of network broadcasts dropped due to an error.

Displaying ICMP Statistics

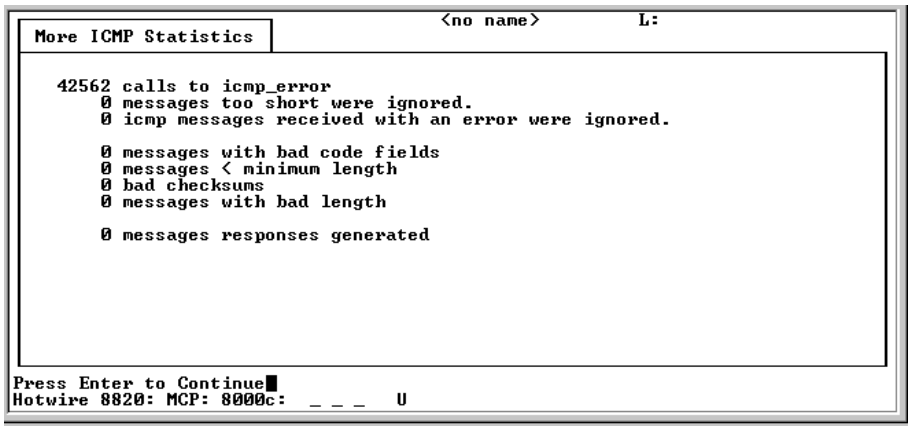
To display information on ICMP statistics, follow this menu selection sequence:

Monitoring → *Network Protocol* → *ICMP Statistics* (**B-D-E**)

The ICMP Packet Statistics screen appears.


<no name> L:
ICMP Packet Statistics
Output Input Status
echo reply 0 0
destination unreachable 4 0
source quench 0 0
routing redirect 0 0 enabled
echo 0 0
time exceeded 0 0
parameter problem 0 0
time stamp request 0 0
time stamp reply 0 0
information request 0 0
information request reply 0 0
address mask request 0 0
address mask reply 0 0
Press Enter to Continue
Hotwire 8810: MCC PLUS: 8000c: _ M _ D

Press Enter to see the second page of ICMP Packet Statistics.


<no name> L:
More ICMP Statistics
42562 calls to icmp_error
0 messages too short were ignored.
0 icmp messages received with an error were ignored.
0 messages with bad code fields
0 messages < minimum length
0 bad checksums
0 messages with bad length
0 messages responses generated
Press Enter to Continue
Hotwire 8820: MCP: 8000c: _ _ _ U

The ICMP Packet Statistics screen displays the information in Table 5-12, ICMP Packet Statistics Screen.

Table 5-12. ICMP Packet Statistics Screen

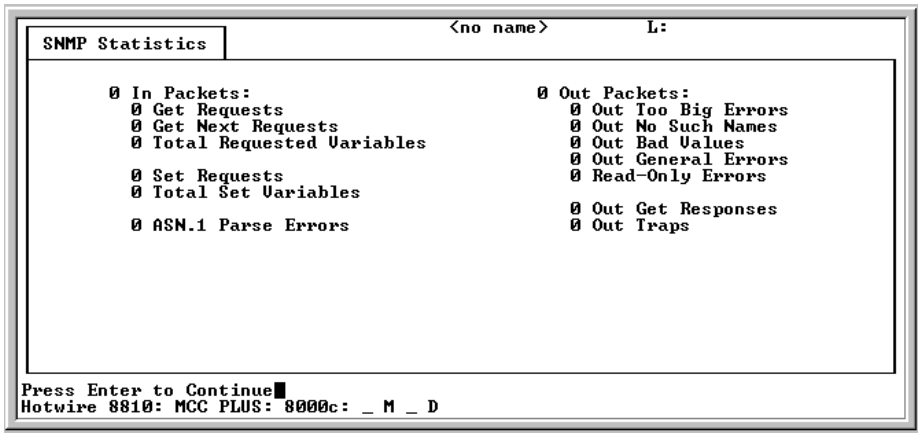
ICMP Packet Statistics	B-D-E
A summary of ICMP activity on all interfaces of the card. The activity is for output and input packets and includes statistics for echo replies, source quench messages, and information requests with their output, input, and status. The Status column is only applicable for “routing redirect.” The counters increment in real time. You may press Ctrl-r at any time to reset them.	

Displaying SNMP Statistics

To display information on SNMP statistics, follow this menu selection sequence:

Monitoring → *Network Protocol* → *SNMP Statistics* (**B-D-F**)

The SNMP Statistics screen appears.



NOTE:

Counters increment in real time. Press Ctrl-r at any time to reset them.

The SNMP Statistics screen displays the information in Table 5-13, SNMP Statistics Screen.

Table 5-13. SNMP Statistics Screen

SNMP Statistics	B-D-F
Displays information on SNMP statistics such as number of set packets, number of get requests, and parsing errors. When you press Enter, the SNMP Authentication Statistics screen displays, giving you additional Community Administration information. **In Packets** – Total number of SNMP Protocol Data Units (PDUs) received by the agent. **Get Requests** – Total number of SNMP Get Request PDUs accepted and processed by the SNMP agent. **Get Next Requests** – Total number of SNMP Get Next PDUs accepted and processed by the SNMP agent. **Total Requested Variables** – Total number of Management Information Base (MIB) retrieved successfully by the SNMP agent as a result of receiving valid SNMP Get Request and Get Next PDUs. **Set Requests** – Total number of SNMP Set Requests PDUs accepted and processed by the SNMP agent. **Total Set Variables** – Total number of MIB objects modified successfully by the SNMP agent as a result of receiving valid SNMP Set Requests PDUs. **ASN.1 Parse Errors** – Total number of ASN.1 or BER errors encountered when decoding received SNMP messages. **Out Packets** – Total number of SNMP PDU responses sent by the agent. **Out Too Big Errors** – Total number of SNMP PDUs generated by the SNMP agent for which the value of error status field is too big. **Out No Such Names** – Total number of SNMP PDUs generated by the SNMP agent for which the value of error status field is “no such name.” **Out Bad Values** – Total number of SNMP PDUs generated by the SNMP agent for which the value of the error status field is bad value. **Out General Errors** – Total number of SNMP PDUs generated by the SNMP agent for which the value of error status is Gen Err. **Read-Only Errors** – Total number of SNMP PDUs delivered by the SNMP agent for which the value of the error status field is read-only. **Out Get Responses** – Total number of Get-Response PDUs sent by the SNMP agent. **Out Traps** – Total number of SNMP Traps PDUs generated by the SNMP agent.	

NOTE:

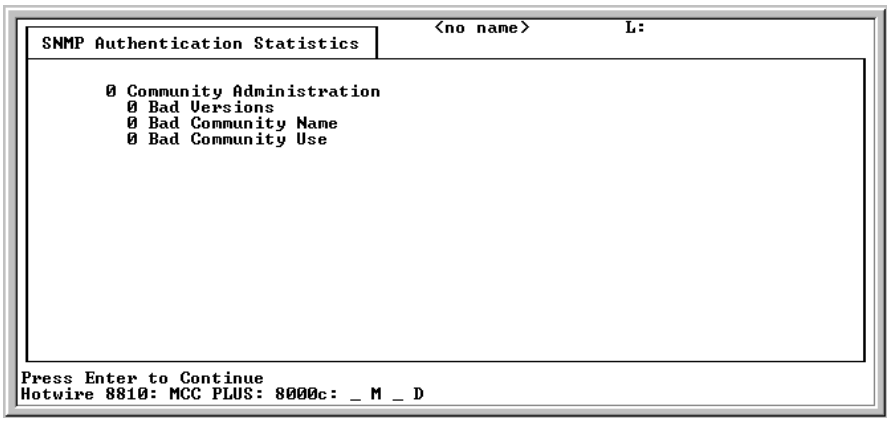
To display additional community administration information, press Enter and the SNMP Authentication Statistics screen appears.

Displaying SNMP Authentication Statistics

You access the SNMP Authentication Statistics screen by following this menu selection sequence:

Monitoring → *Network Protocol* → *SNMP Statistics* (**B-D-F**)

After the SNMP Statistics screen appears, press Enter to access the SNMP Authentication Statistics screen, shown below.



The SNMP Authentication Statistics screen displays the information listed in Table 5-14, SNMP Authentication Statistics Screen.

Table 5-14. SNMP Authentication Statistics Screen

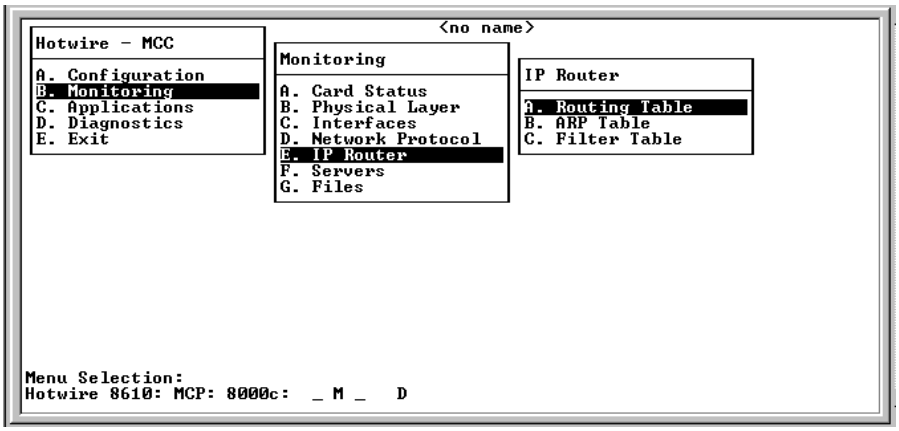
SNMP Authentication Statistics	B-D-F
Community Administration – SNMP PDUs with community-based authentication.	
Bad Versions – Number of SNMP messages delivered to the SNMP agent for an unsupported SNMP version.	
Bad Community Name – Number of SNMP messages delivered to the SNMP agent that used an SNMP community name not known to the entity.	
Bad Community Use – Number of SNMP messages delivered to the SNMP agent that represent an SNMP operation not allowed by the community named in the message.	

IP Router Menu Options

To access the IP Router menu, follow this menu selection sequence:

MCC Main Menu → *Monitoring* → *IP Router* (**B-E**)

The IP Router menu appears.



The IP Router menu provides the following options:

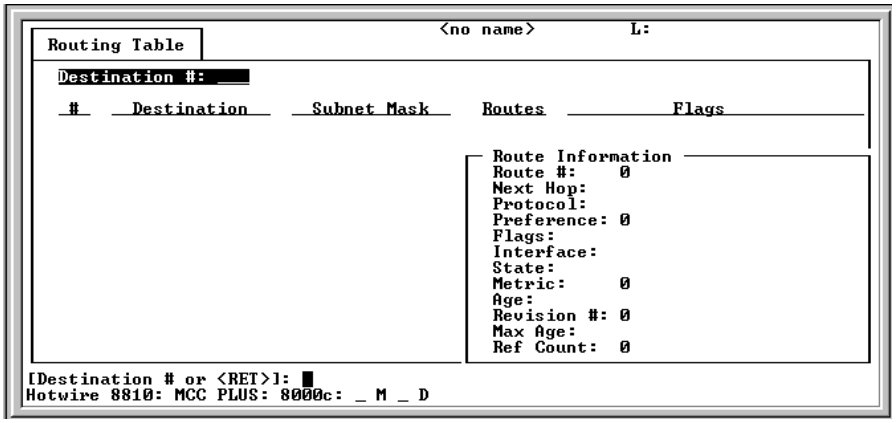
- **A. Routing Table** – Statistics stored in the routing table.
- **B. ARP Table** – The current Address Resolution Protocol (ARP) cache.
- **C. Filter Table** – The various filters that have been configured.

Displaying Routing Table Information and Statistics

To display routing table information and statistics, follow this menu selection sequence:

Monitoring → *IP Router* → *Routing Table* (**B-E-A**)

The Routing Table screen appears.



▶ Procedure

To display information for a specific destination:

1. Type the destination line number at the **[Destination # or <RET>]:** prompt.
2. Press Enter.

   The system displays the working routing table. Routes appear only for active interfaces. The information and statistics are listed by route and destination number. Details for the selected destination are in the lower right corner (Route Information window).

   The Routing Table contains routes to endpoints supported by the diagnostic portal. The portal allows access to the endpoint for troubleshooting. The portal selects the endpoint based on the circuit ID provided, then communicates the IP address to the selected endpoint. The port card establishes a PVC to the endpoint and a session is established. The port card number) and the endpoint's IP Address appear on the Routing Table screen.

   NOTE:

   Select a different destination by typing a number at **[Destination # or <RET>]:** prompt. If more than one route exists for the given destination, view subsequent routes by typing the number at the **Route #:** prompt.

The Routing Table screen displays the information listed in Table 5-15, Routing Table Screen.

Table 5-15. Routing Table Screen

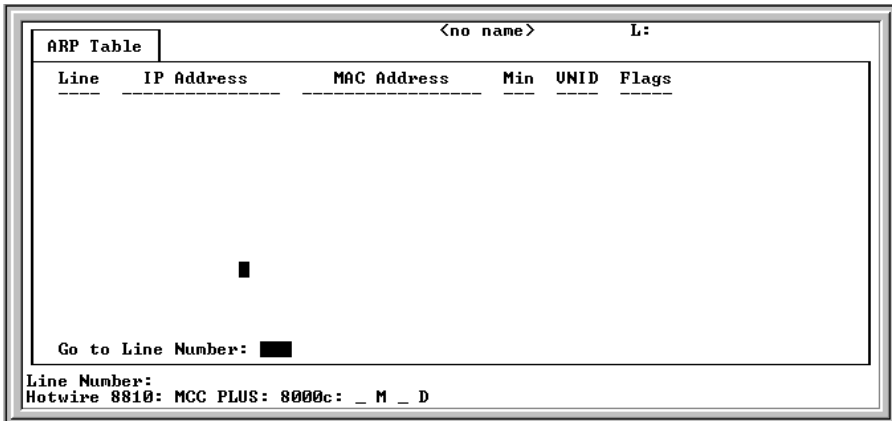
Routing Table	B-E-A
The Routing Table displays the following columns of information: **Routing Table screen** **#** – The entry number in the routing table. Specifies the entry for which you want more information. **Destination** – The destination (or source) IP address of the packet. **Subnet Mask** – The associated subnet mask for the specified destination IP address. **Routes** – Number of routes for Destination. **Flags** – The type of route: host, sub (subnetwork), or net (network).	
Route Information window The lower right-hand corner of the screen displays a Route Information window with detailed information about the selected destination. **Route #** – The number of the route for the given destination. If more than one route exists, view subsequent routes by entering the routing entry number at the **`[Route # or <RET>]:`** prompt. **Next Hop** – The IP address of the next hop device for the specified destination. The port card's slot number appears here for the diagnostic portal PVC to the endpoint. **Protocol** – Type of routing protocol by which the route was learned (i.e., static or direct). **Preference** – The preference number to this route. If more than one route exists, this number is compared to the preference number of the other routes. The value of 0 indicates the highest preference. The greater the number, the lower the preference. **Flags** – Indicates if a route is a Host and if the next hop is valid. **Interface** – The name of the interface associated with the destination address. **State** – The various state information about the route including Permanent, Deleted, SRC, Host, Net, Subnet. **Metric** – Not applicable. **Age** – The length of time in seconds that a non-permanent route has been active. **Revision #** – Not applicable. **Max Age** – Maximum time (in seconds) a non-permanent route has been active. **Ref Count –** Number of internal references for this route.	

Displaying ARP Table Information

To display the current Address Resolution Protocol (ARP) cache, follow this menu selection sequence:

Monitoring → *IP Router* → *ARP Table* (**B-E-B**)

The ARP Table screen appears.



NOTE:

Permanent entries show an age of 0 (zero). There may be more than one page of information. Access additional pages by entering a line number higher than the last number displayed on the current page.

The ARP Table screen displays the information listed in Table 5-16, ARP Table Screen.

Table 5-16. ARP Table Screen

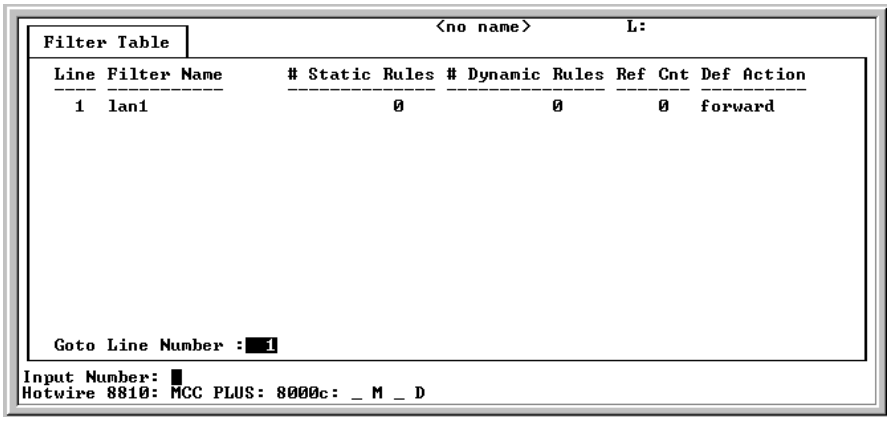
ARP Table	B-E-B
Line – Sequential number of line.	
IP Address – Internet protocol address.	
MAC Address – Media Access Control address.	
Min – Number of minutes since this entry was last used.	
VNID – Not used.	
Flags – Flags associated with the entry. ■ PERM = permanent ■ PUB = publish this entry (respond for other hosts) ■ PROX = proxy ARP (card performs proxy ARP for this IP address)	

Displaying Filters

To display configured filters, follow this menu selection sequence:

Monitoring → *IP Router* → *Filter Table* (**B-E-C**)

The Filter Table screen appears.


Filter Table
<no name>
L:
Line Filter Name # Static Rules # Dynamic Rules Ref Cnt Def Action
1 lan1 0 0 0 forward
Goto Line Number : 1
Input Number:
Hotwire 8810: MCC PLUS: 8000c: _ M _ D

The Filter Table screen displays the information listed in Table 5-17, Filter Table Screen.

Table 5-17. Filter Table Screen

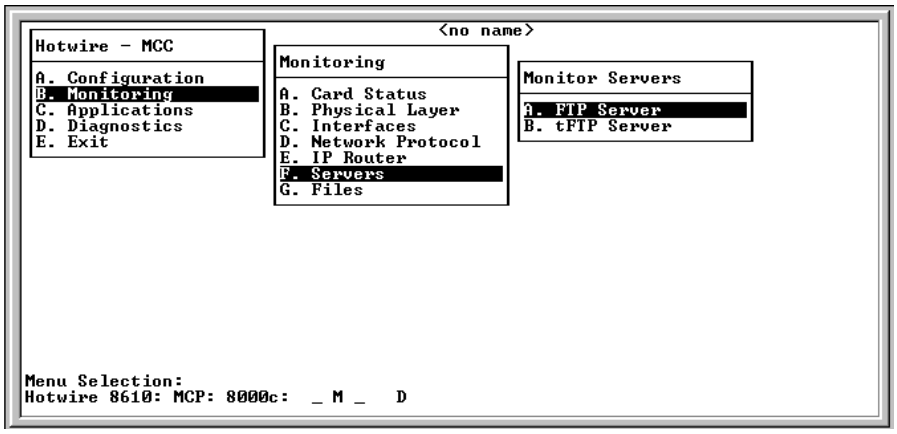
Filter Table	**B-E-C**
Displays the status of the filter.	
Line – Line number.	
Filter Name – Name of the IP filter.	
# Static Rules – Number of static rules in filter.	
# Dynamic Rules – Number of dynamic rules in filter. (Not applicable for MCC.)	
Ref Cnt – Number of active interfaces using this filter.	
Def Action – Default action of filter: Forward/discard.	

Servers Menu Options

To access the Monitor Servers menu, follow this menu selection sequence:

MCC Main Menu → *Monitoring* → *Servers* (**B-F**)

The Monitor Servers menu appears.



The Monitor Servers menu provides the following options:

- **A. FTP Server** – Displays FTP server transactions.
- **B. tFTP Server** – Displays TFTP server transactions.

The Monitor Servers screens display the information listed in Table 5-18, Monitor Servers Screen.

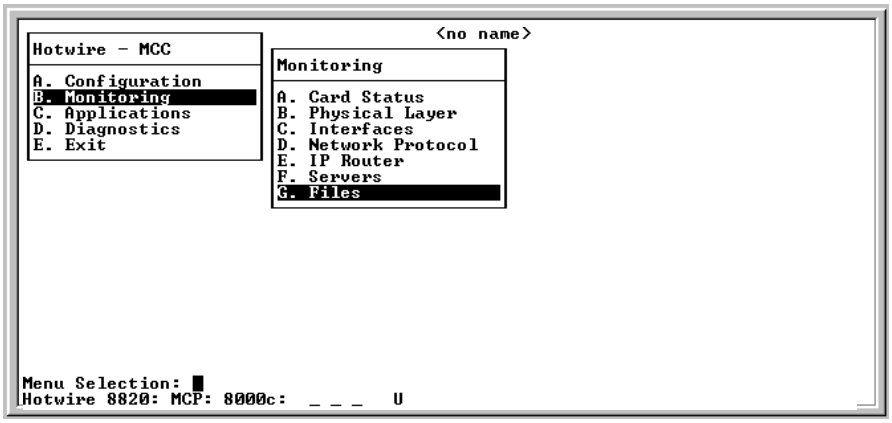
Table 5-18. Monitor Servers Screen

FTP Server	**B-F-A**
Displays the status FTP transactions. **User ID** – Login of the user connected to the FTP server. **Client IP Address** – IP address of the FTP client. **Action** – FTP action (Upload/Download). **Statistics:** **Bytes Transferred** – Number of bytes transferred. **Transfer Time** – Length of time the transfer is taking. **Status** – Status of the file transfer.	
tFTP Server	**B-F-B**
Displays an abstract of the last 30 TFTP file transfers (most recent first). **Slot** – Slot ID of the card to/from which the file is being uploaded/downloaded. **Port** – DSL port number (displayed if the file transfer is to/from an SN accessible from the SN screen). **File Name** – Full path name of the file being transferred. **Action** – TFTP action (Upload/Download). **Statistics:** **Packets Sent** – Number of packets sent. **Packets Received** – Number of packets received. **Bytes Sent** – Number of bytes sent. **Bytes Received** – Number of bytes received. **Transfer Time** – Length of time the transfer is taking. **Status** – Status of the file transfer.	

Files Menu Options

To access the Files menu, follow this menu selection sequence:

MCC Main Menu → *Monitoring* → *Files* (**B-G**)



The Files screen displays the information in the flash file system.

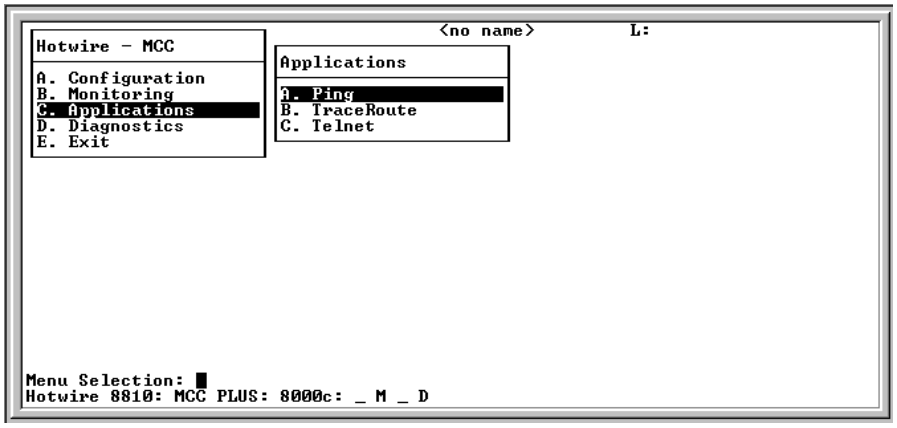
Applications Menu Options

6

Overview

This chapter describes the options on the Applications menu of the MCC card. To access the Applications menu, follow this menu selection sequence:

MCC Main Menu → *Applications* (**C**)



Ping

Ping allows you to conduct a nondisruptive packet test between the MCC and any IP-aware device with network connectivity in the Management domain.

You can ping both upstream and downstream devices. Upstream devices include Network Access and Service Provider routers, switches, and Network Management System (NMS) stations. In the downstream direction, you can ping all Access Nodes in the Hotwire chassis over the backplane as well as TDM SDSL Service Nodes running in IP Complex mode.

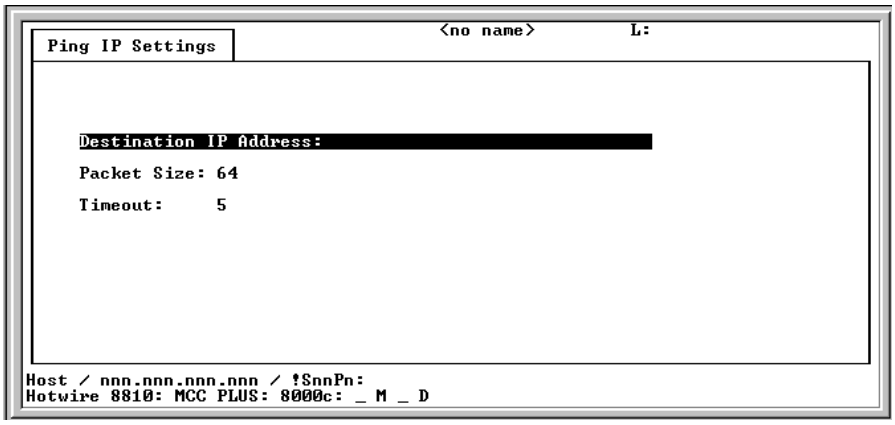
▶ Procedure

To use the Ping function:

1. From the Hotwire – MCC menu, follow this menu selection sequence:

   Applications → *Ping* (**C-A**)

   The Ping IP Settings screen appears.



2. Enter the desired values after each prompt and press Enter.

   — **Destination IP Address:** *nnn.nnn.nnn.nnn* format, or *!SnnPn* format to reach a chassis slot, where *Snn* is the slot number 1 – 18 and *Pn* (in the future) will be for port numbers. For example, to ping the card in Slot 1, enter **!S1**; to ping the card in Slot 10, enter **!S10**.

   — **Packet Size:** 12–1600 bytes (Default = 64).

   — **Timeout:** Wait time before next try. 1–30 seconds (Default = 5).

After the information is entered and Ping is initiated, a results screen displays destination, length, packets sent, timeouts, packets received, the minimum, maximum, and average round trip times of packets, and an incremented list of timeouts after each ping.

NOTE:

The test continues until you exit the screen by pressing Enter.

TraceRoute

TraceRoute displays trace routing information for destinations of up to 64 hops from the MCC card.

NOTE:

You can only use TraceRoute in the upstream direction.

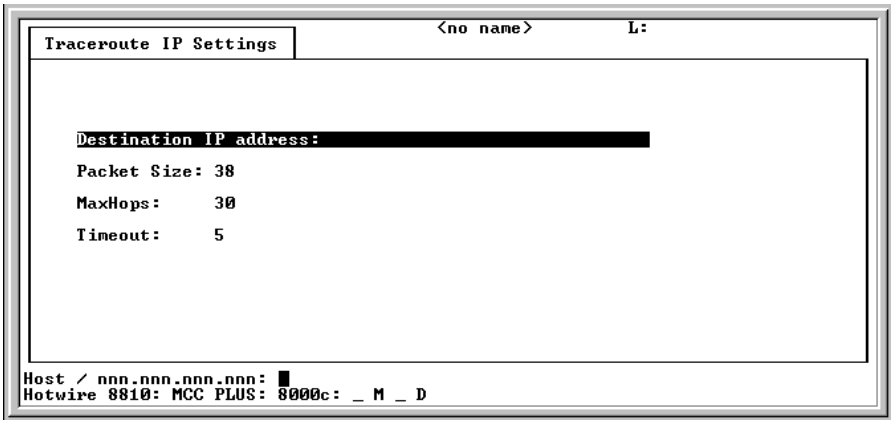
▶ Procedure

To use the TraceRoute function:

1. From the Hotwire – MCC menu, follow this menu selection sequence:

   Applications → *TraceRoute* (**C-B**)

   The TraceRoute IP Settings screen appears.



2. Enter the desired values after each prompt and press Enter.

   — **Destination IP Address:** IP host name or address in *nnn.nnn.nnn.nnn* format.

   — **Packet size:** Length of the packet in bytes (excluding the packet header). 12–1600 bytes (Default = 38).

   — **MaxHops:** Maximum number of hops for trace routing.

   — **Timeout:** Maximum time (in seconds) the system waits before assuming that the packet is lost. 1–30 seconds (Default = 5).

After the above information is entered and TraceRoute is initiated, a results screen displays. Results include destination address, maximum hops, packets sent, timeouts, packets received and a numbered list of reporting hops, each with a number and IP address.

Telnet

Telnet gives you the ability to connect with a remote host or with specific cards in the chassis. You Telnet out (upstream) using IP addresses; you Telnet downstream using slot/part numbers.

NOTE:

You cannot Telnet into the DSL system and then Telnet back out again. Upstream Telnet is only allowed for console access to the DSL cards.

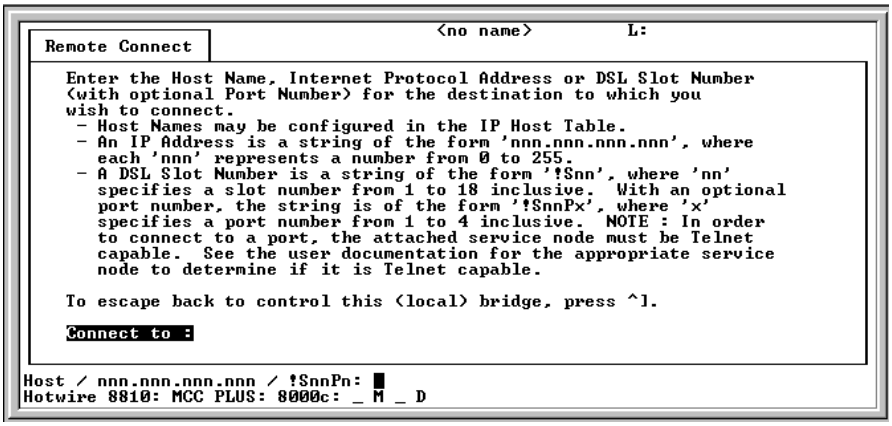
▶ Procedure

To use the Telnet function:

1. From the Hotwire – MCC menu, follow this menu selection sequence:

   Applications → *Telnet* (**C-C**)

   The Telnet (Remote Connect) screen appears.


<no name> L:
Remote Connect
Enter the Host Name, Internet Protocol Address or DSL Slot Number
(with optional Port Number) for the destination to which you
wish to connect.
- Host Names may be configured in the IP Host Table.
- An IP Address is a string of the form 'nnn.nnn.nnn.nnn', where
each 'nnn' represents a number from 0 to 255.
- A DSL Slot Number is a string of the form '!Snn', where 'nn'
specifies a slot number from 1 to 18 inclusive. With an optional
port number, the string is of the form '!SnnPx', where 'x'
specifies a port number from 1 to 4 inclusive. NOTE : In order
to connect to a port, the attached service node must be Telnet
capable. See the user documentation for the appropriate service
node to determine if it is Telnet capable.
To escape back to control this (local) bridge, press ^].
Connect to :
Host / nnn.nnn.nnn.nnn / !SnnPn:
Hotwire 8810: MCC PLUS: 8000c: _ M _ D

2. Enter the desired values after the prompt and press Enter.

   — **Host Name:** IP host name.

   — **DSL IP Address:** IP address in *nnn.nnn.nnn.nnn* format.

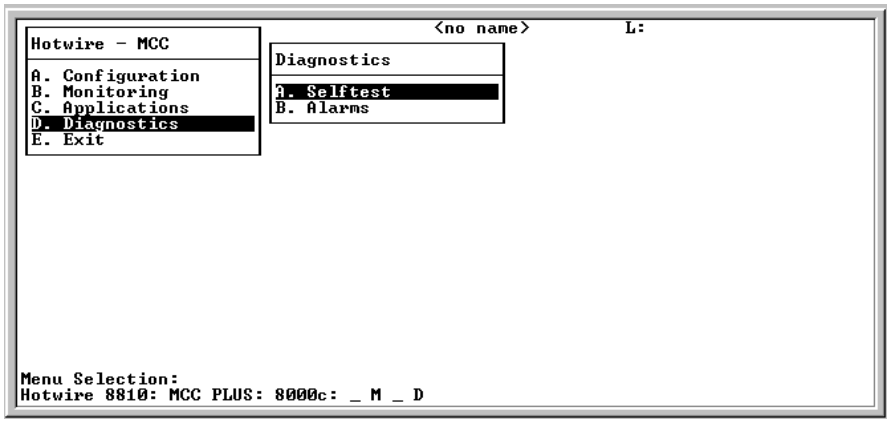
Diagnostics Menu Options

7

Overview

This chapter describes the options on the Diagnostics menu of the MCC card. Use the Diagnostics menu to perform selftests or view alarm status. To access the Diagnostics menu, follow this menu selection sequence:

MCC Main Menu → *Diagnostics* (**D**)



Selftest

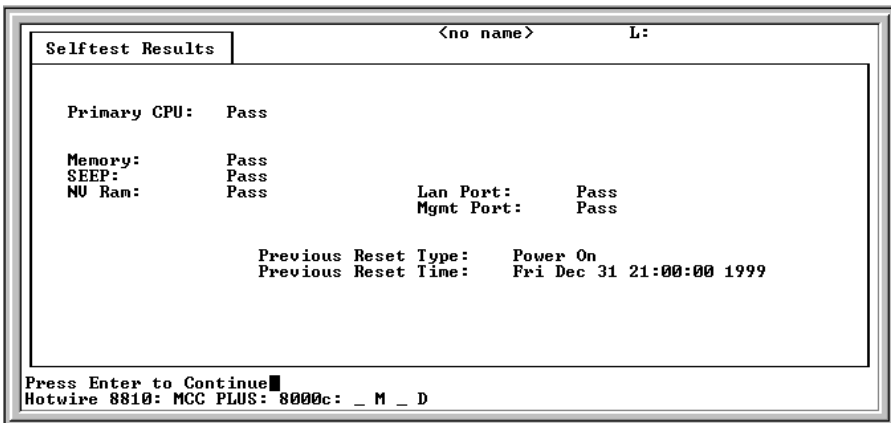
▶ Procedure

To view selftest information:

1. From the Hotwire – MCC menu, follow this menu selection sequence:

   Diagnostics → *Selftest* (**D-A**)

   The Selftest Results screen appears.



   The screen displays the results of the last disruptive selftest of the MCC card. This selftest is only performed on system power-on or a card reset. All subsystems (processors, memory, and interfaces) report pass or fail. If all subsystems pass, the card passes. If a subsystem fails, refer to Chapter 8, *Troubleshooting*, for more information.

Alarm

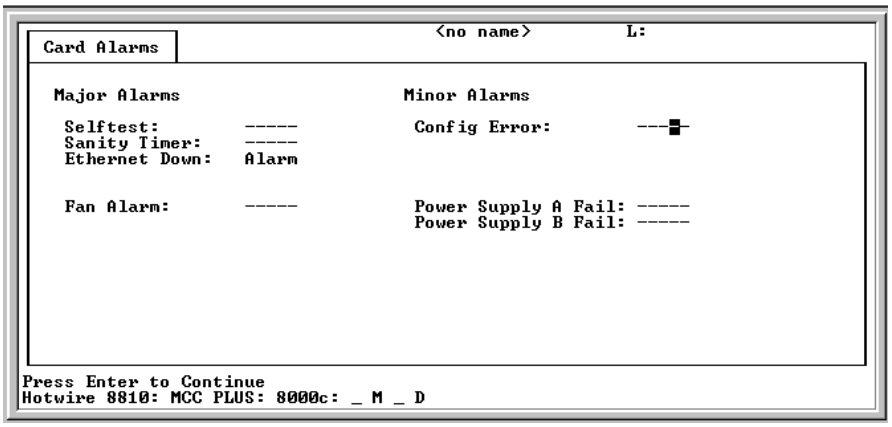
▶ Procedure

To view Alarm information:

1. From the Hotwire – MCC menu, follow this menu selection sequence:

   Diagnostics →*Alarms* (**D-B**)

   The Alarms screen appears.



   The screen displays all active card alarm conditions. Major alarms include Selftest failure, Processor failure (Sanity Timer), and Ethernet failure. Minor alarms include Config Error (configuration has been corrupted).

   For further information about alarms, see Table 8-1, Major Alarms, and Table 8-2, Minor Alarms, in Chapter 8, *Troubleshooting*.

Troubleshooting

8

Troubleshooting the DSL System

Each card in the Hotwire chassis appears on the Quick Card Select screen. The MCC card(s) alone appear on the Mgmt. Card Select screen (see Chapter 2, *Menus and Screens*). Choose either of these selection screens from the Hotwire Chassis Main Menu for MCC card information.

The card is indicated by codes displayed in any of three positions to the right of the card selected. For example:

```
Line 1:    M1(1)  8000  MCP   _ _ _     IP Conserv, Active
Line 2:           Eth(1)      U

Position:                      1 2 3
```

NOTE:

If an option is not active, an underscore appears in its place.

Refer to Table 2-2, Mgmt. Card Select Screen Fields, in Chapter 2, *Menus and Screens*, for an explanation of the codes by position.

Accessing the DSL Cards and Service Nodes (SNs)

All cards in the chassis appear on the Quick Card Select screen. If one or more do not appear, go to the MCC card and follow this menu selection sequence:

Configuration → *Slot* → *Reset Card* (**A-G-A**)

Reset the DSL card by entering its number at the prompt.

▶ Procedure

To select a specific DSL card to reset:

1. From the Hotwire Chassis Main Menu, select one of the following:

   — **A** for Quick Card Select

   — **B** for Port Card Select

   The desired selection screen appears. All active DSL cards appear on either screen.

2. Type the slot number of the DSL card you want to configure, and press Enter.

   The Hotwire — DSL Main Menu appears.

3. Follow this menu selection sequence:

   Configuration → *SN Configuration* (**A-F**)

   The SN Configuration Screen appears.

4. Move the highlight to the **`Reset SN?`** field and enter **yes** at the **`Yes/No:`** prompt. The card resets.

   NOTE:

   Resetting the card temporarily disrupts data on the specified card.

Alarms

If a card selection screen indicates a major or minor alarm on a card, first access the card, then follow this menu selection sequence to determine the cause of the alarm:

Diagnostics → *Alarms* (**D**-**B**)

NOTE:

If a DSL card does not appear on a card selection screen because the MCC card can no longer communicate with it, the MCC card generates an error message. On the MCC card, go to *Monitor* → *Card* → *Syslog* (**B-A-C**) and view the event on the system log.

Major Alarms

Use Table 8-1, Major Alarms, to determine the appropriate action for each major alarm.

Table 8-1. Major Alarms

Failure Type	Action
Selftest failure	1. Check the Selftest Results screen by following the menu sequence: *Diagnostics* → *Selftest* (**D-A**). 2. Do another Selftest (Reset) and check results. – If results are normal, the problem was transient. Log the results. – If results are the same, pull the card out and plug it in again. Check all connections. Do another Reset and check results. – If results are the same as the first selftest, replace the card.
Processor failure (Sanity timer)	1. Do another Selftest (Reset) and check results. – If results are normal, the problem was transient. Log the results. – Review the syslog for additional information. – If results are the same, pull the card out and plug it in again. Check all connections. Do another Reset and check results.
Ethernet Down	1. Check cable connections to the chassis. – If cables are terminated properly, go to Step 2. – If cables are not terminated properly, terminate them correctly. 2. Check cable connections to the Ethernet Hub. – If cables are terminated properly, go to Step 3. – If cables are not terminated properly, terminate them correctly. 3. Check the Activity/Status LED at the Ethernet Hub. – If Activity/Status LED does not indicate a problem, go to Step 4. – If Activity/Status LED indicates a problem, take appropriate action. 4. Disconnect the Ethernet cable and replace it with a working cable from a spare port on the Hub. – If the replacement cable works, the original is bad. Replace it. – If the replacement cable does not work, the MCC card is probably bad and should be replaced.
Fan Alarm	Check the system fan and its connections. If it is not functioning, replace it.
Non-Supported Chassis	The chassis does not support this card. Check that the card is in the proper chassis (8600, 8610, 8800, 8810, 8620, or 8820).

Minor Alarms

Use Table 8-2, Minor Alarms, to determine the appropriate action to take for each Minor Alarm.

Table 8-2. Minor Alarms

Failure Type	Action
Config Error	1. Check the Selftest Results display by following the menu sequence: *Diagnostics* → *Selftest* (**D-A**). 2. Do another Selftest (Reset) and check results. – If the results are normal, the problem was transient. Log results. – If Selftest results still show configuration corruption, there is a card problem. The card's nonvolatile RAM should be erased and the configuration reentered. Perform a configuration download. – If the configuration has not been saved, use reset and erase NVRAM to force the card to the factory default. Enter the basic default route to the MCC and reconfigure the card manually.
Power Supply A Fail	Check power supply A and its connections. If it is not functioning, replace it.
Power Supply B Fail	Check power supply B and its connections. If it is not functioning, replace it.

Management Domain Problems

To provide a practical aid in the isolation and resolution of Layer 3 network difficulties, the guidelines in this section provide information on troubleshooting a generic network containing the devices found in most networks. This section addresses potential problems that may occur in the MCC Card-to-Router (or NMS) segment of the network. For troubleshooting other network segments, refer to the *Hotwire MVL, ReachDSL, RADSL, IDSL, and SDSL Cards, Models 8310, 8312/8314, 8510/8373/8374, 8303/8304, and 8343/8344, User's Guide*.

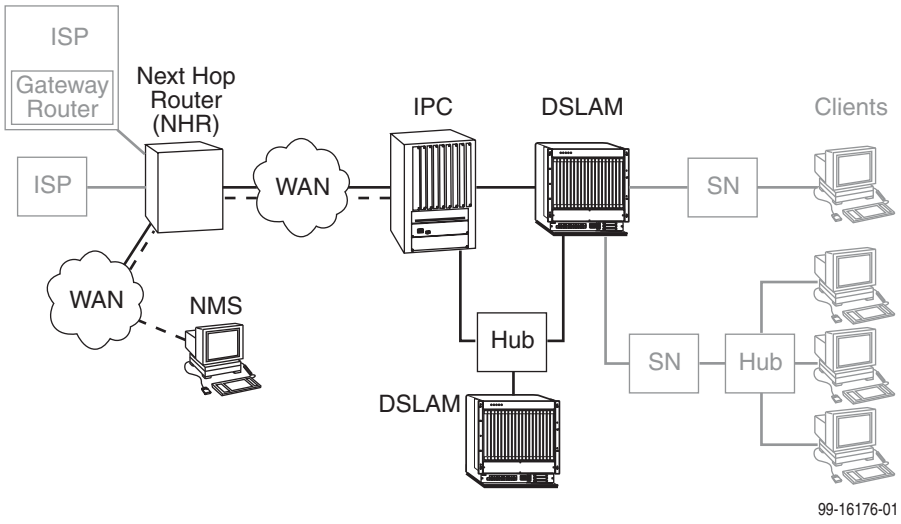
These procedures assume that Asynchronous Transfer Mode (ATM) is used on the link between the IPC and the next hop router (NHR).

High-Level Troubleshooting

The following high-level procedures help you isolate problems to a particular segment of the network.

- Make sure the MCC's default gateway is the same as the IP address for the appropriate ISP router.
- An Address Resolution Protocol (ARP) table may have invalid entries if a recent configuration change took place anywhere on the network and not enough time has passed for the entry to expire. Check the ARP tables on the client, DSL system, and router.
- Make sure a default route is configured on the MCC card (screen **A-E-A**).

The following figure shows a generic network addressed in this section.



MCC Card Cannot Ping Next Hop Router

Table 8-3. MCC Card-to-Next Hop Router Segment

Checklist Type	Solution
Layer 1 – Physical	If the Alrm LED on the MCC is lit, go to screen **D-B** to determine the cause(s). A major alarm such as Ethernet usually means there is no Ethernet connection between the MCC port on the chassis and the IPC. Check the cable and make sure the pinouts are correct.
	If a Hotwire 8610 chassis (three slots) is being used, make sure the MCC Ethernet cable is plugged into the port labeled MCC, the Ethernet port labeled 1 is not used, and the daisy dial is set to 1 (on the base unit). The 3-slot chassis can be daisy-chained for user expandability.
	If hubs are used, make sure the cabling is correct.
	To view the MCC card self-test results, go to screen **D-A**. The screen shows faults in the card's processor, memory, and interfaces.
	Go to the system log (screen **B-A-C**) and check system failures.
	Check all cabling to make sure there is a link between the MCC card and the IPC.
Layer 2 – Network	Make sure a default route is configured on the MCC card (screen **A-E-A**).
	Make sure the MCC Ethernet port is part of a virtual port, not an 802.1Q (VNID) group.
	Make sure the correct IP address is configured (screen **A-C-B**). Enter **eth1** for the Ethernet interface and view or edit the IP address. Reset the card if changes are made. The MCC address can only be configured statically.

MCC Cannot Ping NMS Server

Table 8-4. MCC Card-to-Network Management System (NMS) Segment

Checklist Type	Solution
Layer 1 – Physical	Make sure a link is up between the NMS and the DSL system. A Cat 5 cable must be plugged into the MCC port on the chassis and the NMS device.
	Make sure the NMS is functional.
Layer 2 – Network	On the NMS, make sure the IP address is correctly configured.
	If the NMS is on a different subnetwork, make sure its IP address is known to the router through either dynamic or static routing protocols.
	On the MCC card (screen **A-F-A**) make sure the NMS IP address for traps is correctly configured. If SNMP security is enabled, go to screen **A-F-A** and make sure the server IP address is correctly configured.

Performance Issues – Viewing Network Statistics

The previous sections examined connectivity issues, i.e., the inability to Ping the router. Table 8-5, Examining Performance Issues, presents information on viewing DSL statistics screens to examine performance issues. You are now looking at performance in the data domain. You must first access the port card to see this information.

Table 8-5. Examining Performance Issues

To . . .	Go To . . .
View Statistics	Any statistics screen. These screens give information related to the number of packets transmitted and received on an interface as well as any packet failures. ■ To view Ethernet statistics, go to screen **B-B-B**. ■ To view HDLC statistics, go to screen **B-B-C**. ■ To view error statistics, go to screen **B-B-F** and choose a port. ■ To view transmit statistics, go to screen **B-B-G** and choose a port. ■ To view system log, go to screen **B-A-C**.
Examine Slow Performance	Screen **B-B-B**. Slow performance could result from errors seen on this screen. Make sure the MCC card and IPC are both operating at either full or half-duplex mode. On the MCC card, go to screen **A-B-A**. On the IPC, enter **10/100cfg**. If operating at full-duplex, a hub should not be used.
Examine Collisions	Screen **B-B-B**. Minimal collisions are acceptable if packets are not being discarded. Excessive collisions could result from forcing too much data over a single Ethernet.

Recovering from a Failed Download

If the download process fails, the system remains in Download mode. To recover from this, you must restart the download. See Appendix A, *Upgrade Procedures*, for download procedures.

Recovering from a Failed Login Attempt

If you are denied access during a Telnet session, the session stops and an error is logged. If you are using a console, return to the User Login screen.

If you forget your password, contact the Paradyne Technical Service Center. Have the serial number of the MCC card available, and the service representative will provide you with a password.

Upgrade Procedures

A

Upgrade Instructions Overview

The upgrade procedures are essential because portions of new software may be incompatible with earlier versions. If the procedures are not followed exactly, you can permanently lose communication with the port cards (ANs) and endpoints (SNs) and it will be necessary to visit these locations to resolve the problem. The port card and the MCC card must be at the same GranDSLAM release version for full feature compatibility.

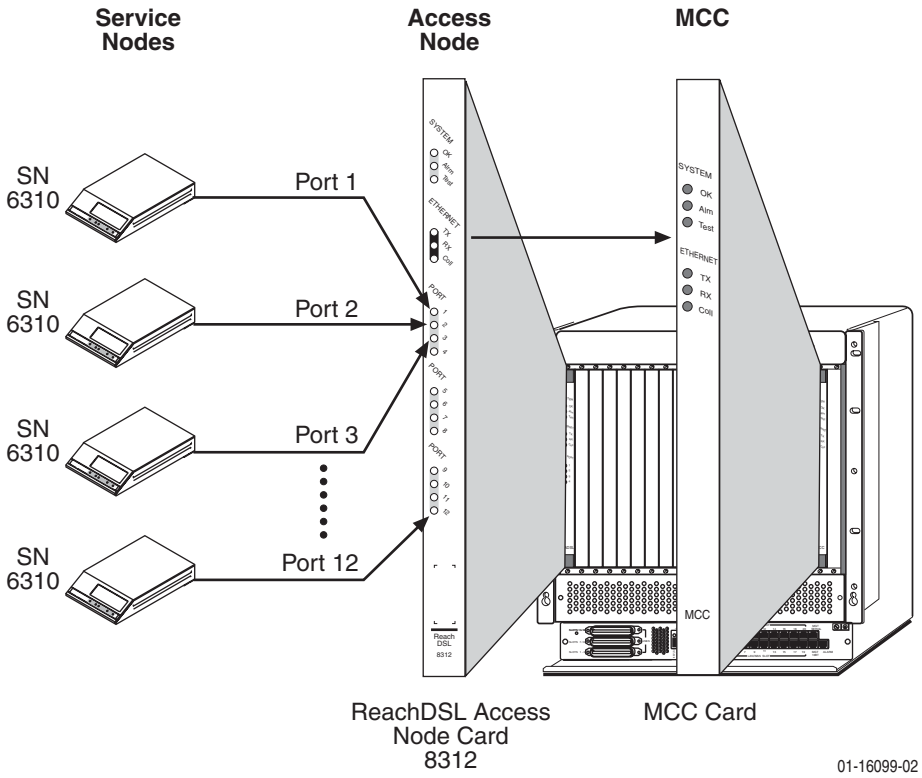
For TDM SDSL/SHDSL devices, refer to the appropriate device manual listed in the *Product-Related Documents* section in *About This Guide*.

NOTE:

The following instructions are *essential* to a successful upgrade. All procedures *must* be followed exactly.

Firmware Download Sequence

Use the download function of the MCC card (*Configuration → Card → Download Code*) to download new version of firmware to the components of the DSL system.



For All Cards (Except ReachDSL)

New firmware must be downloaded to the following in the order listed for all cards (except ReachDSL):

1. All endpoints (SNs) connected to a specific port card (AN).
2. The port card from Step 1.
3. All port cards and their connected SNs (repeat Steps 1 and 2).
4. The Management Communications Controller (MCC) card.

The SCM card can be downloaded at any point in the process.

For ReachDSL Cards

ReachDSL cards must be downloaded in the following order:

1. The Management Communications Controller (MCC) card.
2. All ReachDSL cards.
3. All endpoints (SNs).

Accessing Firmware/Software Files

To copy the DSL firmware files to your server, you must have subscribed to the Paradyne Technical Support Program.

▶ Procedure

1. Access **www.paradyne.com**.
2. Select *Support → TSP Subscribers.*
3. Log in to the Paradyne Technical Support program.
4. Select *Subscriber Firmware*.
5. From the Paradyne Firmware/Software (Subscriber) Files Download Page, select *Hotwire GranDSLAM x.x Products* and download the appropriate firmware versions for your network environment.

Firmware Version Numbers

The Hotwire DSL network includes the components:

- IPC
- MCC Card (MCC, MCP, MCC Plus)
- SCM Card (Hotwire 8620/8820 GranDSLAM chassis only)
- 8373/8374/8510 RADSL Cards
- 8310 MVL Cards
- 8312/8314 ReachDSL v1 (formerly MVL) Cards
- 8312/8314 ReachDSL v2 Cards
- 8303/8304 IDSL Cards
- 8343/8344 SDSL Cards
- 8335/8365/8385 ATM Cards
- TDM SDSL/SHDSL Cards

- Endpoints
  - — 5620 RTU
  - — 6310 ReachDSL v1 (formerly MVL) Modem
  - — 6301 IDSL Router
  - — 6302 IDSL Router
  - — 6341 SDSL Router
  - — 6342 SDSL Router
  - — 6350 ReachDSL v2 Modem
  - — 6351 ReachDSL Router
  - — 6371 RADSL Router

For a list of the most up-to-date firmware version numbers, check the Paradyne Firmware/Software Subscriber Files Download Page. For proper functionality, each component must use the listed (or higher) version of firmware.

NOTES:

- — When you install the first 8312 12-port ReachDSL card in the chassis, verify that the 6310 SN firmware is at a minimum version level of 04.01.01. If it is not, you must download the new firmware so that the 6310 SN is compatible with 8312 ReachDSL firmware.
- — Be aware that to upgrade to 8510 firmware release 2.0 from versions earlier than 8546 release 02.03, you must first upgrade to release 02.03.

Firmware Upgrade Procedures

Three methods of upgrading firmware to the SCM, MCP and port cards are available:

- Files can be stored on a PC or workstation and manually downloaded to the card (see *Manual Firmware Download* on page A-5).
- Files can be stored on the MCP's Flash File System (FFS) and manually downloaded to the card (see *Manual Firmware Download* on page A-5 and *MCP Flash File System* on page A-7).
- Files can be stored on the MCP's FFS and automatically downloaded to the card (see *Automatic Firmware Download* on page A-12).

Manual Firmware Download

Use the Download Code screen (**A-A-G-A**) to download firmware. The fields of the Download Code screen are defined in the following table.

Field	Description	Input
Download Type	Firmware to be downloaded. **NOTE:** If you enter SN, fields for slot # and Port # appear; if you enter PC, a field for Slot # appears.	MCC, SCM, PC, or SN
Card/Slot #	Slot number of the port card to which the code is downloaded. Only appears if PC or SN is entered in Download Type field.	Slot numbers 1–18
SN Connected to Port #	Port number to which the Service Node is attached. Only appears if SN is entered in Download Type field.	Port numbers
Immediate Apply	Specifies whether the card automatically resets upon completion.	Yes or No
Image File Name	File to be downloaded. May be a path name ending with the file name. The file can reside on a PC/workstation or on the MCP's FFS. If the TFTP server is hosted by a DOS machine running other than Windows 2000 or Windows NT, then directory and file names must follow the 8.3 DOS convention.	Total path name must be fewer than 40 characters
tFTP Server IP Address	The Host name or IP address of the TFTP server or M1 if using the MCP FFS.	*Host /nnn.nnn.nnn.nnn* format
Start Transfer	Specify whether you want to start the transfer.	Yes or No (Default = No)

Downloading New Firmware

Use this procedure to download new code.

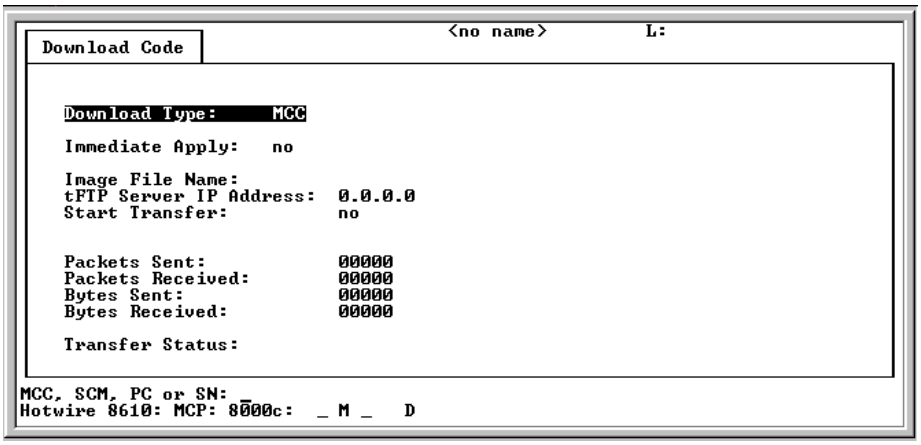
▶ Procedure

To download new firmware from the MCC card:

1. Follow this menu selection sequence:

   Configuration → *Card* → *Download Code* → *Download Code* (**A-A-G-A**)

   The Download Code screen appears and the **`Download Type:`** field is highlighted.



2. At the **MCC, SCM, PC or SN:** prompt, enter the device to which you are downloading code.

   If you entered **PC**, a field for Slot # appears. If you entered **SN**, fields for Slot # and Port # appear.

3. If downloading to a port card, enter port card's chassis slot number at the **Card/Slot #:** prompt, then press Enter.

   If downloading to a Service Node, enter the slot number of the port card to which the SN is connected at the **Card/Slot #:** prompt, then press Enter. The **SN Connected to Port #** field is highlighted. Enter the port number to which the SN is attached.

   The **Immediate Apply:** field is automatically set to yes and the **Image File Name:** field is highlighted.

4. At the **Image File Name:** prompt, enter the complete path name for the upgrade file on your server and press Enter.

5. At the **Enter File Name:** prompt, enter the complete path name for the upgrade file on your server and press Enter.

   NOTE:

   You must have the updated files on your server. These files are available from the Paradyne Web site.

   The **tFTP Server IP Address:** field is highlighted.

6. At the **Host/nnn.nnn.nnn.nnn:** prompt, enter the IP address of your server on which the upgrade file is stored (or M1 if using the MCP FFS) and press Enter.

   The **Start Transfer:** field is highlighted.

7. At the **`yes/no:`** prompt, type **yes** to begin the process.

   `Transfer in progress` appears and the following fields begin to increment:

   Packets Sent – Number of packets sent in download.

   Packets Received – Number of packets received in download**.**

   Bytes Sent – Number of bytes sent in download.

   Bytes Received – Number of bytes received in download.

   When the transfer completes, the Transfer Status field changes to **`Completed successfully.`** The SN or card resets and connectivity is reestablished.

   NOTES:

   — When an SN has completed the upgrade, communication with *all* of its end users is enabled.

   — The SN resets and may lose connectivity until its port card is upgraded.

8. Repeat the procedures for all Service Nodes and port cards in your DSL system.

If you cannot communicate with an SN after a complete upgrade of the SN and port card, verify firmware level compatibility and retry the firmware download. If you are upgrading a 6341/6342 SDSL Router from firmware older than 3.1.4, you must upgrade to version 3.1.7, upgrade the port card, then upgrade the router to the current release.

MCP Flash File System

A file system which can be used to store the configuration of the SCM, MCP, and port cards in a Hotwire GranDSLAM is available for firmware release M04.00.38 and above. This flash file system (FFS) can also be used to store firmware files which can then be downloaded to the SCM, MCP, and port cards. The FFS is contained on the MCP card menu *Configuration* → *Files* → *File System* (**A-I-A**).

Two types of directories are used in the FFS. The firmware (fw) directory contains the code image software for downloading port and management cards. The configuration directories (slot_a, slot_1, etc.) are used to store GranDSLAM card configurations and firmware files.

Uploading Files to the MCP's FFS

Use this procedure to upload firmware files to the MCP card's FFS via FTP.

▶ Procedure

To upload new firmware to the MCP card from a host PC:

1. At the DOS prompt **`C:\>`**, FTP to the MCP card by typing **ftp** and the MCP card's IP address, then press Enter.
2. At the **`User:`** prompt, type the MCP password, then press Enter. Or just press Enter if no password has been defined for the MCP card.
3. After receiving confirmation of your log-in, type **bin** at the **`ftp>`** prompt to transfer binary data, then press Enter.
4. At the **`ftp>`** prompt, type **hash** to display hash marks (**#**) on the screen so that you can follow the progress of the upload, then press Enter.
5. At the **`ftp>`** prompt, type **put** followed by the local directory and name of the file you are transferring. Then type a space followed by the MCP firmware directory to which you are uploading the file and the name you are giving the file (can be different from its current name). Then, press Enter.

   For example:

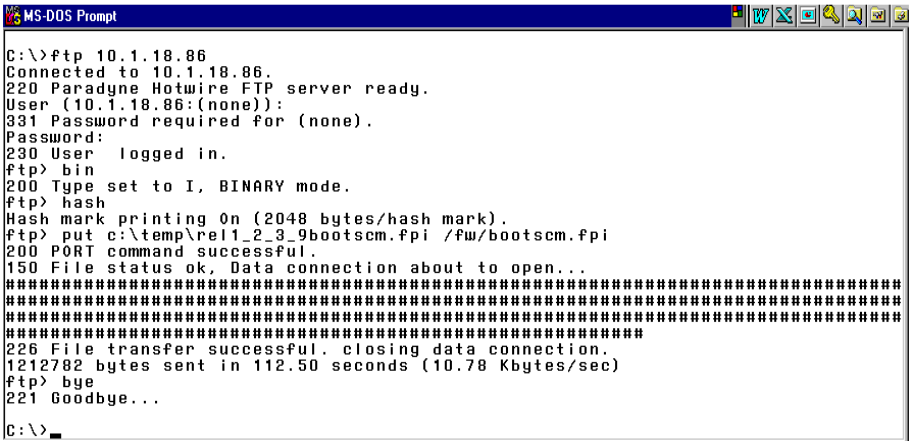
   `put c:\temp\rel1_2_3_9bootscm.fpi /fw/bootscm.fpi`

   The screen displays hash marks indicating the progress of the file transfer.

   After the hash marks have stopped appearing on your screen and you receive confirmation that your file transfer was successful, type **bye** at the **`ftp>`** prompt, then press Enter.

   The session is ended.

   The following screen is an example of transferring an SCM image file to the FFS.


MS-DOS Prompt
C:\>ftp 10.1.18.86
Connected to 10.1.18.86.
220 Paradyne Hotwire FTP server ready.
User (10.1.18.86:(none)):
331 Password required for (none).
Password:
230 User logged in.
ftp> bin
200 Type set to I, BINARY mode.
ftp> hash
Hash mark printing On (2048 bytes/hash mark).
ftp> put c:\temp\rel1_2_3_9bootscm.fpi /fw/bootscm.fpi
200 PORT command successful.
150 File status ok, Data connection about to open...
226 File transfer successful. closing data connection.
1212782 bytes sent in 112.50 seconds (10.78 Kbytes/sec)
ftp> bye
221 Goodbye...
C:\>

NOTE:

You can also monitor the progress of the FTP file transfer with the FTP Server screen (**B-F-A**).

Verifying Firmware Upload to the MCP's FFS

Use this procedure to verify that firmware files to the MCP card's FFS was successful.

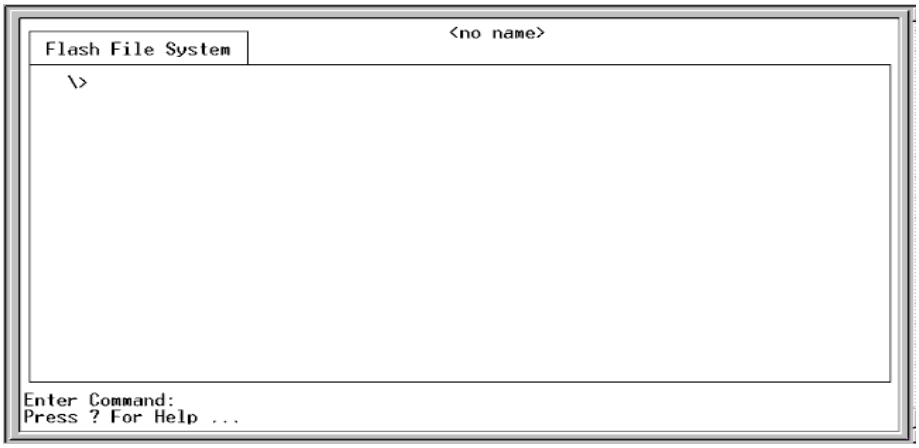
▶ Procedure

To verify the upload of firmware to the MCP card:

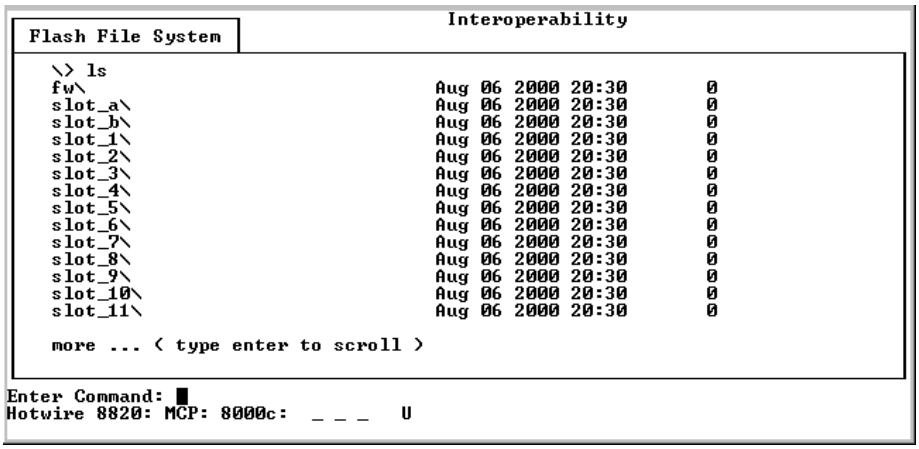
1. Telnet to the MCP card.
2. Select the MCP card from either the Quick Card Select or Mgmt. Card Select screen off the Hotwire Chassis Main Menu.
3. From the MCP's main menu, follow this menu selection sequence:

   Configuration → *Files* → *Files System* (**A-I-A**)

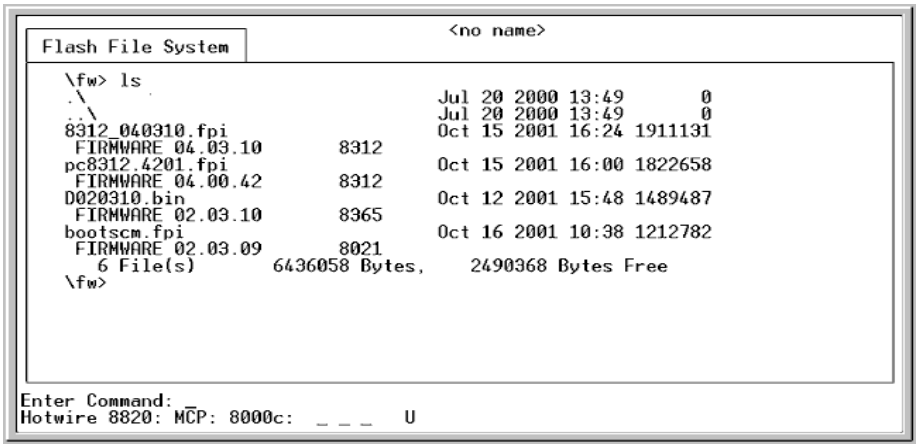
   The Flash File System screen appears.



4. At the **`Enter Command`** prompt type **ls** or **dir** to list the MCP directory, then press Enter.


Interoperability
Flash File System
\> ls
fw\ Aug 06 2000 20:30 0
slot_a\ Aug 06 2000 20:30 0
slot_b\ Aug 06 2000 20:30 0
slot_1\ Aug 06 2000 20:30 0
slot_2\ Aug 06 2000 20:30 0
slot_3\ Aug 06 2000 20:30 0
slot_4\ Aug 06 2000 20:30 0
slot_5\ Aug 06 2000 20:30 0
slot_6\ Aug 06 2000 20:30 0
slot_7\ Aug 06 2000 20:30 0
slot_8\ Aug 06 2000 20:30 0
slot_9\ Aug 06 2000 20:30 0
slot_10\ Aug 06 2000 20:30 0
slot_11\ Aug 06 2000 20:30 0
more ... (type enter to scroll)
Enter Command:
Hotwire 8820: MCP: 8000c: _ _ _ U

5. At the **`Enter Command`** prompt type **cd fw** to switch to the firmware directory on the MCP card where the firmware file was saved during the upload, then press Enter.
6. At the **`Enter Command`** prompt type **ls** or **dir** to view the firmware files stored in this directory, then press Enter. You should see the name of the file you FTPed to this directory during the firmware upload.



Once the firmware files are stored in the FFS, they can be downloaded to the port cards (see *Manual Firmware Download* on page A-5 and *Automatic Firmware Download* on page A-12).

Saving a Card Configuration

Use TFTP to save a configuration to the FFS. The NVRAM Cfg Loader screen (**A-A-E**) enables you to TFTP the file to the appropriate system file directory.

▶ Procedure

To save a configuration to the MCC card's FFS:

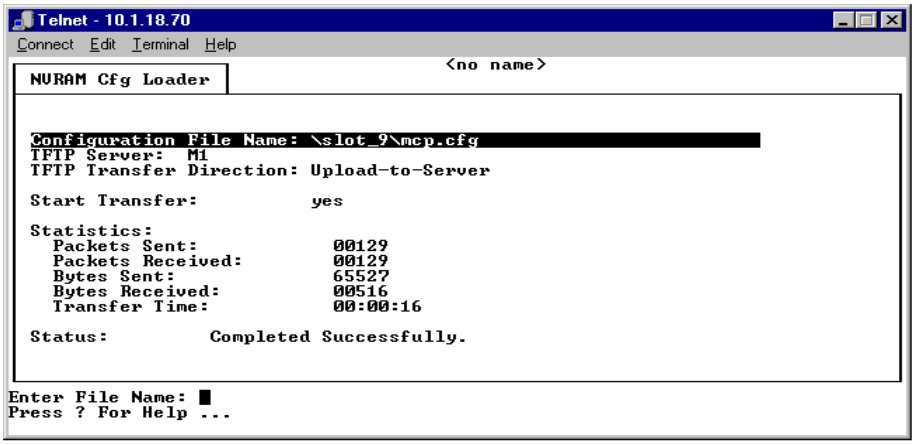
1. Use the NVRAM Config Loader screen to upload configurations to and download the MCC's configuration from a Trivial File Transfer Protocol (TFTP) server. Follow this menu selection sequence:

   Configuration → *Card* → *NVRAM Cfg Loader* (**A-A-E**)

   The NVRAM Cfg Loader screen appears.

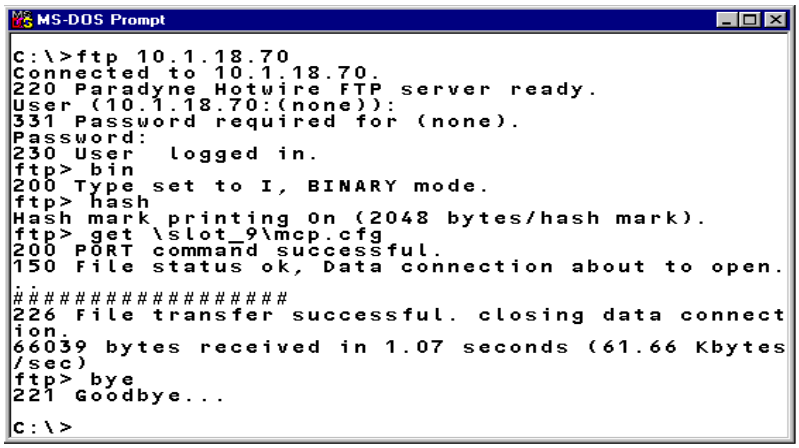
2. Type the desired value in each field and press Enter. The TFTP Transfer direction is Upload-to-Server for saving a configuration (or use Download-from-Server to restore the card's configuration). The TFTP Server IP Address is the IP address of the MCC card.

3. When the transfer completes, the Transfer Status field changes to **`Completed successfully.`**



Saving MCC Card Configurations to a Host Computer (PC)

Once you have stored GranDSLAM card configurations in the FFS, they can be retrieved from the MCP and saved on the PC. To do this, use FTP on the PC changing the directories to the one containing the desired file, then do a “get” to retrieve the file.



Automatic Firmware Download

Version 04.03.*xx* or greater of the MCC card allows you to automatically download firmware files stored in the MCC card’s Flash File System (FFS) to cards in the GranDSLAM. When a port card is detected in the GranDSLAM slot (either by power-on or reset), the MCP will determine if a download is required and initiate one if determined necessary. Firmware will be automatically downloaded only if the firmware stored in the FFS is different (older or newer) than the firmware on the card, and if the Automatic Firmware Download feature has been enabled. If you install a new card or replace an old one, the card will automatically be downloaded with firmware installed in the MCP’s FFS. This ensures that all cards of the same type will have the same firmware version. In addition, Automatic Firmware Download simplifies upgrading an entire GranDSLAM. A firmware file can be transferred via FTP into the fw directory, then the port cards are reset. Once the port cards have been reset, the new firmware is automatically downloaded to them.

NOTE:

Endpoint firmware is not automatically upgraded.

Prior to version 4.03.*xx*, the MCP’s FFS allowed multiple firmware files in its fw directory, but only one file in the slot_*n* directory (*n* equals the slot number). The only file allowed in the slot_*n* directory was the card’s configuration file. With firmware version 04.03.*xx*, firmware files can also be stored in the slot_*n* directory.

Automatic Firmware Download enables you to load firmware to a card from either the fw directory or the slot_*n* directory. All port cards as well as the SCM card can be automatically downloaded; however the MCP card cannot be automatically downloaded. Multiple cards can be downloaded at the same time. If the SCM card is included, it is downloaded first so that the uplink will be available for the port cards.

For more information on Automatic Firmware Download, see *Files Menu* in Chapter 4, *Configuration Menu Options*.

Downloading Firmware in slot_*n* Directory

When a port card or the SCM card completes a reset (whether by reseating the card, or by UI/SNMP command, or by replacing the card) the automatic firmware feature (if enabled) will first look for a firmware file in the slot_*n* directory for that card. If a firmware file is found and it is compatible yet different than the firmware installed on the card in that slot, then the firmware will be downloaded (even if the firmware file is older than the firmware installed on the card). If there are multiple compatible firmware files in the slot_*n* directory, then the most recent one will be downloaded.

If after a reset no firmware file is found in the slot_n directory, then the Automatic Firmware Download feature will look in the fw directory. If a compatible yet different firmware file is found, then that firmware will be downloaded (even if the firmware file is older than the firmware on the card that is installed in that slot). If there are multiple compatible firmware files in the fw directory, then the most recent one will be downloaded.

Cards can be upgraded or downgraded. Downgrading firmware may cause NVRAM to be cleared on the card being downgraded. Firmware release numbers have 3 sets of digits (xx.yy.zz). If there is major release change (difference in the xx or yy digits) between the firmware that is on the card and the firmware to be loaded, then the NVRAM will be cleared after it has been downgraded. Always save configuration files from the MCP card in case you need to restore your configurations. If the downgrade is a minor release change (only zz changes), then an NVRAM clear will not be done.

CAUTIONS:

— The Automatic Firmware Download feature is completely automatic. You will not be prompted for permission to download. Therefore, you must ensure that the correct firmware is installed in the proper directories if you enable this feature.

— It is important to delete any unused firmware files to conserve space. Enter **ls** or **dir** from the FFS to display the bytes available.

— Firmware should typically be stored in the fw directory. Placing firmware in the slot_*n* directory is a special situation.

Download Examples

- **Upgrading all cards of the same type**

  For example, if the GranDSLAM has Model 8365 cards in slots 1 through 8 which are running build 02.03.10, build 02.03.10 resides in the fw directory of the FFS, and there is no firmware in the slot_1 through slot_8 directories. To upgrade to build 02.03.11, simply FTP build 02.03.11 into the fw directory and reset the cards in slots 1 through 8. When the cards complete the reset, build 02.03.11 will be downloaded to those cards.

- **Upgrading only one card**

  Allowing firmware to be stored in both the slot_*n* and fw directories allows you to store different versions of firmware for the same type of card in different slots. For example, if you have multiple Model 8314 cards, all the cards are running with build 04.03.10, and you also have build 04.03.10 installed in the fw directory of the FFS. A new build of firmware becomes available for Model 8314 (04.03.11). If you want to test this firmware on only one card (for example, the card in slot 1), then you would place build 11 in the slot_1 directory of the FFS and reset the card in slot 1. Upon completion of the reset, the automatic download feature would see that there is a different build in the slot_1 directory than what is on the card and download build 11.

  If you want to revert back to the old firmware (build 10), then just delete build 11 from the slot_1 directory and reset the card in slot 1. After the reset, the Automatic Firmware Download feature will check the slot_1 directory and find no firmware. Because there is no firmware in the slot_1 directory, it will then check the fw directory. It finds build 10 in the fw directory and downloads that firmware to the card in slot 1 (downgrading from build 11 to build 10). Since this was a minor release downgrade of code, it will NOT send an NVRAM clear to that slot. If, however, this was a major release downgrade of code, then NVRAM would be cleared on the card. See the cautions in *Downloading Firmware in slot_n Directory* on page A-13.

IP Filtering Overview and Worksheets

B

Overview

This appendix provides an overview of packet filters, and worksheets to help plan and record your filter configurations. All filters are set on the MCC card.

A filter is used to:

- Secure a network by implementing security rules
- Prevent unauthorized network access without making authorized access difficult.

By default, MCC filtering is not active on the Hotwire DSL system. However, you can enable filtering to selectively filter source or destination packets being routed through the MCC card. Use the worksheets provided later in this appendix to help you plan and record your filter configurations.

What is a Filter?

An **IP filter** is a rule (or set of rules) that is applied to a specific interface to indicate whether to forward or discard a packet.

A filter works by successively applying its rules to the information obtained from the packet header until a match is found. (Host rules have precedence over network rules.) The filter then performs the action specified by the rule on that packet: forward or discard. If the packet header information does not match any rules, then the user-specified default filter is used. The filter does not change any state or context, and the decision is based only on the packet header.

You can create the following filter types:

- An **input filter** to prevent packets entering the MCC card through an e1a interface from being forwarded. You may want to set up filtering on input to protect against address spoofing. Use the IP Network screen (*Configuration* → *Interfaces* → *IP Network*) to bind an input filter to a particular interface.
- An **output filter** to prevent packets from going out of the MCC card through an e1a interface. Use the IP Network screen (*Configuration* → *Interfaces* → *IP Network*) to specify binding of an output filter to a particular interface.

For each filter type, you must set up one or more of the following rule types on the IP Filter Configuration screen (*Configuration → IP Router → IP Router Filters*):

- A **network address rule type** to discard or forward packets/traffic from a specified network or network segment. This rule type enhances security by allowing access only to certain networks. The IP address and subnet mask specified in the **`Destination address`** and **`Destination address mask`** fields, or the **`Source address`** and **`Source address mask`** fields of the IP Filter Configuration screen are compared to the destination/source address contained in the IP header of the packet.
- A **host address rule type** to discard or forward packets/traffic from a specified host. This rule type can also be used to enhance security by allowing access only to certain hosts. The IP address and subnet mask specified in the **`Destination address`** and **`Destination address mask`** fields, or the **`Source address`** and **`Source address mask`** fields of the IP Filter Configuration screen are compared to the destination/source address contained in the IP header of the packet.

  NOTE:

  Host address rules have precedence over network address rules.

- A **socket address rule type** to limit certain applications. This rule type is used primarily when filtering TCP and UDP packets, and may be used in conjunction with a network address rule type or a host address rule type. The destination (socket) port number specified in the **`Destination Port No.`** field and source (socket) port number specified in the **`Source Port No.`** field of the IP Filter Configuration screen are compared to the destination and source port numbers in the TCP and UDP header of the packet.

  NOTE:

  If both the source and destination port numbers are 0s (zeros), the system filters ICMP packets in addition to the packet types defined in the rule.

You can configure up to two filters on the MCC card. Also, up to 33 rules can be configured for each filter. Keep in mind that you need to configure the default filter action (forward or discard packets) for each filter.

For detailed information on the IP Filter Configuration screen and the IP Network screen, see Chapter 4, *Configuration Menu Options*.

IP Filtering Configuration Worksheets

This section provides worksheets to assist you in creating filters. Use the worksheets to record filter parameters such as IP filter types and rule types for the MCC card. Photocopy the worksheets as needed.

Summary: How to Define a Filter

To define a filter for a specific interface to indicate whether a packet can be forwarded or discarded on that interface:

- Go to the appropriate IP Filter Configuration screen to define a filter and set up one or more rule types (network address rule type, host address rule type, and/or socket address rule type) for that filter.
- Go to the appropriate IP Network screen to bind the filter (i.e., specify the filter type (input filter or output filter) by specifying the name of the filter in the appropriate field and binding it to a specific interface).

  NOTE:

  For the MCC card, **lan1** (bound to e1a) is the default filter.

  When using lan1 as the input, by default, lan1 is already bound to its corresponding interface (e1a). To use lan1 as the output filter, you must manually bind it on the IP Network screen.

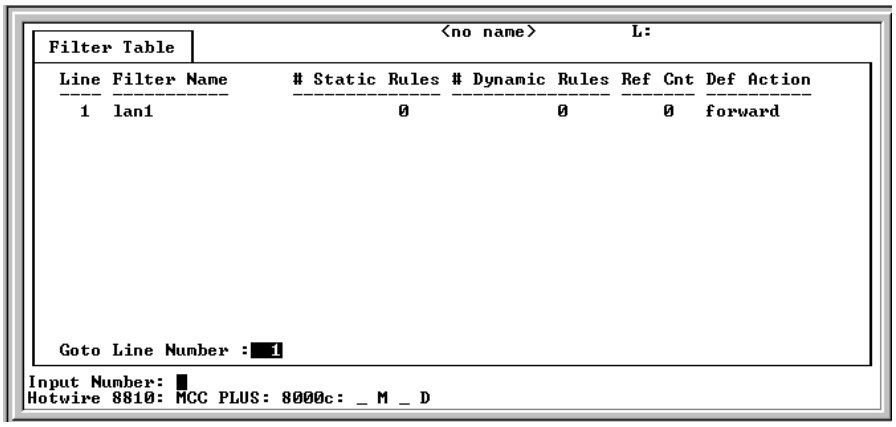
Worksheet: Defining the Filter and Rules

On the IP Filter Configuration screen, create a filter and define its rules. Complete one worksheet for each rule.

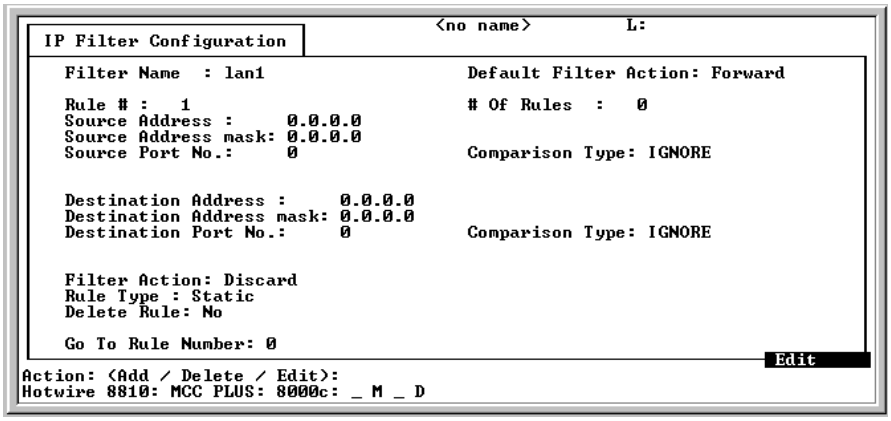
NOTE:

Up to 33 rules can be configured for each filter. If you do not specify rules, the system forwards or discards packets based on the value set for the default filter action (on the **`Def Action`** field). By default, this field is set to forward.

Select *Configuration* → *IP Router* → *IP Router Filters* from the Hotwire – MCC menu to display the Filter Table screen.


Filter Table
<no name> L:
Line Filter Name # Static Rules # Dynamic Rules Ref Cnt Def Action
1 lan1 0 0 0 forward
Goto Line Number : 1
Input Number:
Hotwire 8810: MCC PLUS: 8000c: _ M _ D

Enter the line number of the desired filter name on the Filter Table screen to display the IP Filter Configuration screen.



IP Filter Configuration	A-E-C
Prompt	**Your Configuration Setting**
1. At the **`Action: (Add/Delete/Edit):`** prompt, type **A** to add a rule.	
2. At the discard/forward: prompt, type the desired filter action.	Default Filter Action =
3. Enter the name of the filter for which you want to define rules at the **`Enter Filter Name:`** prompt. The DSL system provides a default filter, **lan1**, for the MCC card. **lan1** is already bound to the e1a interface. **NOTE:** You cannot delete the default filter name from the system. But you can specify another filter by overwriting the existing name. If you change the filter, remember to change the name in the **`Input Filter`** field on the IP Network screen. The default filter name is bound to the e1a interface.	Filter Name =

IP Filter Configuration *(Continued)*	A-E-C
Prompt	**Your Configuration Setting**
4. Depending on the rule type(s) you want to use, do one or more of the following: – To define a *network address rule type*, specify either an IP address or subnet mask in the **`Source Address`** and **`Source Address mask`** fields, or the **`Destination Address`** and **`Destination Address mask`** fields. – To define a *host address rule type*, specify either an IP address or subnet mask in the **`Source Address`** and **`Source Address mask`** fields, or the **`Destination Address`** and **`Destination Address mask`** fields. – To define a *socket address rule type*, specify the source (socket) port number at the **`Source Port No.`** field and the destination (socket) port number at the **`Destination Port No.`** field. This rule type may be used in conjunction with a network address or host address rule type. **NOTE:** Host address rules have precedence over network address rules. All host address rules are invoked sequentially before the first network rule. If defining a socket address rule type, you must also specify the comparison type you want to perform in the Comparison Type field. Enter **IGNORE** if you do not want to do a comparison, or one of the following to do a comparison on the port number specified in the packet and the rule: **EQ** (equal to), **NEQ** (not equal to), **GT** (greater than), **LT** (less than), **IN_RANGE** (within the specified range), **OUT_RANGE** (outside of the specified range).	**Rule #** ____ Source Address = Source Address mask = Source Port No. = Comparison Type = Destination Address = Destination Address mask = Destination Port No. = Comparison Type =
5. Enter **forward** at the **`Filter Action:`** prompt to activate filtering for the specified filter name, or **discard** to prevent packets that match the rule(s) from passing through.	Filter Action =

Worksheet: Binding the Filter

On the IP Network screen, indicate whether you want to use the filter you just defined on the IP Filter Configuration screen as an input or an output filter for a specific interface.

NOTE:

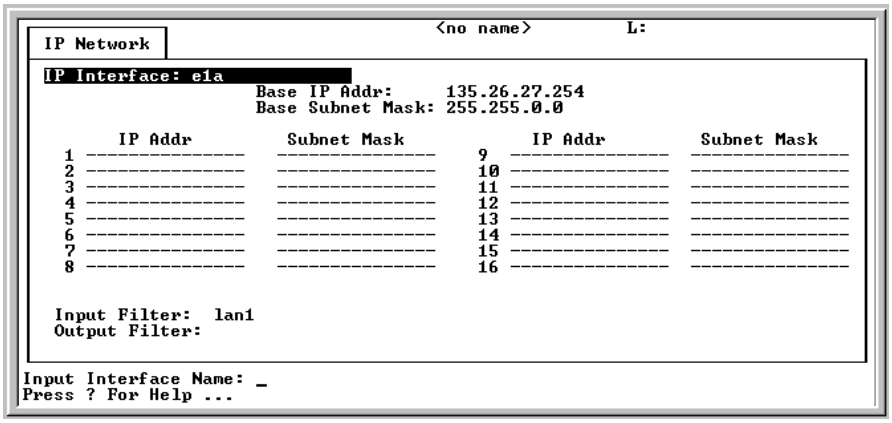
When using the default input filter name (lan1), you do not need to complete a worksheet. The default filter name is already bound to its corresponding interface (e1a), and no further action is required.

However, you need to complete the following worksheet if you:

— Changed the default input filter name on the IP Filter Configuration screen, or

— Defined an output filter and that filter needs to be bound to a specific interface.

Select *Configuration* → *Interfaces* → *IP Network* from the Hotwire – MCC menu to display the IP Network screen.



IP Network Screen	
Prompt	**Your Configuration Setting**
1. Enter the interface name (e1a) at the **`Input Interface Name:`** prompt.	IP interface = e1a
2. Enter *one* of the following: – For the Input Filter field, enter the desired filter name at the **`Filter Name (blank to disable filtering):`** prompt. Use an input filter to prevent packets entering the DSL card through an e1a interface from being forwarded. – For the Output Filter field, enter the desired filter name at the **`Filter Name (blank to disable filtering):`** prompt. Use an output filter to prevent packets from going out of the DSL card through an e1a interface.	Input Filter = or Output Filter = **NOTE**: If you are using the default filter name as the input filter, the filter is already bound to the e1a interface.

Input Screens

C

MCC Card Input Screens

Table C-1, MCC Card Input Screens, provides an alphabetical listing of all MCC screens. The screens are listed by the name that appears in the “tab” in the upper-left corner of the screen. The right column contains the menu selection sequence by which you access the screen.

Table C-1. MCC Card Input Screens (1 of 2)

Screen Name	Menu Selection Sequence
Access Restriction	Configuration → Access Security Access Restriction (**A-D-C**)
Active Interfaces List	Monitoring → Interfaces → Active List (**B-C-A**)
Active Ports List	Monitoring → Physical Layer → Active List (**B-B-A**)
Add ARP Entry	Configuration → IP Router → ARP → ARP Entry (**A-E-D-B**)
Apply Code	Configuration → Card → Download Code → Apply Code (**A-A-G-B**)
ARP Parameters	Configuration → IP Router → ARP → Parameters (**A-E-D-A**)
ARP Table	Monitoring → IP Router → ARP Table (**B-E-B**)
Auto Code Download	Configuration → Files → Auto Code Download (**A-I-B**)
Card Alarms	Diagnostics → Alarms (**D-B**)
Card Information	Configuration → Card→ Card Info (**A-A-A**)
Card Reset	Configuration → Card → Card Reset (**A-A-F**)
Configuration Backup/Restoral	Configuration → Files → Cfg Backup/Restore (**A-I-C**)
Configure DNS	Configuration → Card → DNS Setup (**A-A-B**)
Control Interfaces	Configuration → Interfaces → Control (**A-C-C**)
Download Code	Configuration → Card → Download Code → Download Code (**A-A-G-A**)
Ethernet Ports	Configuration → Ports → Ethernet Port (**A-B-A**)
Ethernet Statistics	Monitoring → Physical Layer → Ethernet Stats (**B-B-B**)
File System	Configuration → Files → File System (**A-I-A**)

Table C-1. MCC Card Input Screens (2 of 2)

Screen Name	Menu Selection Sequence
File System	Monitoring → Files → File System (**B-G-A**)
Filter Table	Configuration → IP Router → IP Router Filters (**A-E-C**)
Filter Table	Monitoring → IP Router → Filter Table (**B-E-C**)
FTP Statistics	Monitoring → Servers → FTP Statistics (**B-F-A**)
General Card Information	Monitoring → Card → Card Info (**B-A-A**)
ICMP Packet Statistics	Monitoring → Network Protocol → ICMP Statistics (**B-D-E**)
IDSL Clock Configuration	Configuration → Slot → IDSL Clock Setup (**A-G-B**)
Interfaces	Configuration → Interfaces → General (**A-C-A**)
Interface Status	Monitoring → Interfaces → Status (**B-C-B**)
IP Host Table	Configuration → IP Router → Host Table (**A-E-E**)
IP Network	Configuration → Interfaces → IP Network (**A-C-B**)
IP Statistics	Monitoring → Network Protocol → IP Statistics (**B-D-D**)
Login History	Monitoring → Card → Login History (**B-A-B**)
Martian Networks	Configuration → IP Router → Martian Networks (**A-E-B**)
NVRAM Cfg Loader	Configuration → Card → NVRAM Cfg Loader (**A-A-E**)
NVRAM Clear	Configuration → Card → NVRAM Clear (**A-A-D**)
Ping IP Settings	Applications → Ping (**C-A**)
Radius Security	Configuration → Access Security → Radius Security (**A-D-B**)
Reset Card	Configuration → Slot → Reset Card (**A-G-A**)
Remote Connect (Telnet)	Applications → Telnet (**C-C**)
Routing Table	Monitoring → IP Router → Routing Table (**B-E-A**)
Selftest Results	Diagnostics → Selftest (**D-A**)
SNMP Communities/Traps	Configuration → SNMP → Community/Traps (**A-F-A**)
SNMP Statistics	Monitoring → Network Protocol → SNMP Statistics (**B-D-F**)
Socket Statistics	Monitoring → Network Protocol → Socket Statistics (**B-D-A**)
Static Routes	Configuration → IP Router → Static Routes **(A-E-A**)
Syslog	Configuration → Syslog (**A-H**)
Syslog	Monitoring → Card → Syslog (**B-A-C**)
TCP Data Statistics	Monitoring → Network Protocol → TCP Statistics (**B-D-C**)
TFTP Statistics	Monitoring → Servers → TFTP Statistics (**B-F-B**)
Time/Date	Configuration → Card → Time/Date (**A-A-C**)
TraceRoute IP Settings	Applications → TraceRoute (**C-B**)
UDP Statistics	Monitoring → Network Protocol → UDP Statistics (**B-D-B**)
User Accounts	Configuration → Access Security → User Accounts (**A-D-A**)

Remote Access

D

Accessing the MCC Card through a Modem

To access the MCC card through a modem, follow the procedure below. It is assumed that all hardware and cabling connections are properly established.

NOTE:

Use of the hardware listed below, and the following procedure, may not work in all environments.

▶ Procedure

To access the MCC through a dial-in modem.

1. Use a Paradyne 7612 modem (or compatible).
2. At the modem end of the connection, use a null modem and a 25-pin-to-8-pin adapter connected to the serial jack of the Hotwire chassis.
3. Dial in from a terminal with VT100 emulation. Use RADIUS Authentication (**A-D-B**).
4. Configure your terminal or terminal emulator with the following settings:
   - — Baud Rate = 9600
   - — Data Bits = 8
   - — Parity = No Parity
   - — Stop Bits = 1
   - — Flow Control = XON/XOFF
   - — Terminal Type = VT100

Simple Network Management Protocol

E

SNMP Overview

The Simple Network Management Protocol (SNMP) is an application-level protocol used in network management to gather information from network devices. Each device runs an SNMP agent that collects data. A Network Management System (NMS), such as Paradyne's OpenLane®, communicates with the SNMP agent on the MCC card to obtain specific parameters or variables.

SNMP agents are located on the MCC card and the Access Node (AN) or port card. The Service Node (SN) devices are managed through a proxy agent on the AN.

Managed SN devices can be set up as remote and/or central devices for TDM SDSL cards:

- **Remote** – Statistics are collected by the SN at the customer premises
- **Central** – Statistics are collected by the AN at the central office

Most communication between the NMS and the MCC card originates with a request message (Get) from the NMS to the MCC card. When the MCC card receives the SNMP Get request, the SNMP agent transmits a response (positive or negative) to the NMS. When certain significant events occur within the SNMP agent, they can result in transmission of unprompted SNMP trap messages to the NMS.

Community Structures

You direct SNMP requests to DSL system logical entities through the MCC card by the use of community structures. The community structure is based on a slot and interface numbering scheme. There are two sections of the community structure:

- Security string – the current community string
- Locator string – indicates the physical location

In the community structure the security string and locator string are separated by an "at" symbol (@). An example of a community structure is:

`public@s14`, where s14 is the slot number.

The default, read-only string "public" allows MCC users with access permission to view information in the MIBs unless the customer changes the default values or institutes the security features.

The MCC agent parses the community structure for the "@" symbol. When it is found, the appended characters are tested to determine if they are a valid locator string. If the locator string is valid, the security string is authenticated. Community structures for each slot are stored by the Entity MIB on the MCC agent.

Default SNMP community names for each access level are pre-assigned in order to partition access to MIB information. They cannot be changed through a SNMP MIB but can be changed via the MCC terminal interface or a Telnet session.

All DSL cards must support IP conservation, in which only one external IP address is assigned to the chassis, and specific cards are identified by a suffix to the community string. This suffix identifies the slot number in which the card resides. The suffix may also include a port number tag to identify a SN.

The four default community string names are:

- public – read-only
- mcc – read/write
- nms – read/write
- nms-2 – read-only

Each community string name can be assigned one of the following permissions:

- ReadOnly
- ReadWrite
- NoAccess

SNMP Gets and Sets

An SNMP “get” allows the management station to retrieve an object value from a managed station.

To enable the “set” capability, the NMS manager needs the correct Read/Write (R/W) community name. If security is enabled, the NMS manager’s IP address must be specified with R/W privileges on the SNMP Security screen. This applies only to MCC card SNMP security.

NOTE:

Before entering the IP address of the TFTP server, you must SNMP “set” the configuration file name.

Settable Objects

Objects that can be set are listed below:

- SNMP Authentication Failure Trap
- All objects in ipNetToMedia Table
- System Name, Location, and Contact in MIB II Systems Group
- System Reset
- Start Configuration Download

  You can do an SNMP “set” for an object corresponding to the file name and IP address of the TFTP server. If the SNMP-initiated configuration download succeeds, the DSL card resets after the download and a CCN trap is sent. If the SNMP-initiated configuration download fails, a failure trap is sent. These traps are sent only if they have been configured on the SNMP Communities/Traps screen.
- Start Configuration Upload
- DSL or MCC card Reset from MCC
- Clear Statistics Registers

Traps

Traps inform the NMS of an alert occurring in the system (e.g. threshold exceeded). They are sent at the start and completion of a test or alarm condition.

Traps are configured via a Telnet or terminal session and are based on community names. Traps are included in the MIB II, entity and Hotwire enterprise MIB definitions.

The DSL system can send traps to three IP addressable destinations (e.g. NMS, printer) per community (for a total of 12 destinations).

All generic (i.e., link up/down, warm start) and standard traps (MIB specific) are supported as they apply to the system. The transmission of generic traps is enabled/disabled by the Network Access Provider using the NMS.

The addition of a DSL card in the DSL system causes a New Card Detected Trap to be generated. The MCC sends a configuration change notification trap (CCN) to indicate a hardware replacement or software upgrade to a card, or the removal of a card.

MCC Traps

Table E-1 lists some of the traps generated by the MCC card. Additional traps are in the Paradyne DSL Enterprise MIBs. MIBs can be accessed through the Paradyne Web site at **www.paradyne.com**. Select *Support →Technical Information → MIBS.*

Table E-1. MCC Card Traps

Event	Severity	Comment	Trap #	MIB
A power source failure	minor	Power source A has failed and the hot_sys.mib (Hotwire system) is now operating off one source.	10	hot_sys.mib (Hotwire system)
A power source normal	normal	Power source A is now operating normally.	110	hot_sys.mib (Hotwire system)
Authentication failure	minor	SNMP community string mismatches.	4	MIB II (RFC 1213)
Authentication failure	minor	Telnet and terminal password mismatches. This trap may be overloaded for terminal and Telnet based auth failures. In these cases the following is also sent with the trap PDU: – Access mode used – Number of auth failures For SNMP-based failures, no information is sent.	8	hot_sys.mib (Hotwire system)

DSL Traps

SNMP defines six MIB II traps. The Access Node SNMP agent defines five traps and does not support trap messages with a value of 5. These messages are identified with a value of 0 through 5 in the generic-trap field of the trap message. The specific-trap field of standard trap messages is set to 0 (zero). The specific-trap field of enterprise-specific messages defines the trap. Some of the traps are enterprise traps and some are MIB II traps.

Table E-2 lists some of the traps generated by the DSL cards.

Table E-2. DSL Card Traps (1 of 3)

Event	Severity	Comment	Trap #	MIB
CCN (Configuration Change Notice)	warning	Configuration change caused by one the following events: ■ software download ■ configuration download ■ card removed (objective)	7	hot_sys.mib (Hotwire system)
CCN (Configuration Change Notice)	warning	Configuration change caused by a change affecting the entity MIB	1	hot_domain.mib (Enterprise domain)
Cold start	warning	Card has been reset and performed a cold start.	0	MIB II (RFC 1213)
Configuration download failure	warning	Configuration download has failed.	2	hot_diag.mib (Hotwire diagnostics)
Device failure	major	AN's operating software has detected an internal device failure.	15	hot_sys.mib (Hotwire system)
DHCP file security failure	minor	Host table is full (has reached a maximum of 32 entries in the client table).	11	hot_dhcp.mib (Hotwire DHCP Relay Agent)
xDSL port failure	major	Processor detected bad DSL modem chip set.	5	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL link up or down Transitions threshold exceeded	minor	Number of link down events above threshold. This rate is limited to once every 15 minutes.	1	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL margin low	minor	Margin estimate below customer set threshold.	3	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL margin normal	normal	Margin estimate now above customer set threshold.	103	hot_xdsl.mib (Hotwire XDSL Interface)

Table E-2. DSL Card Traps (2 of 3)

Event	Severity	Comment	Trap #	MIB
xDSL port speed low	warning	Port speeds decreased to lower bound thresholds.	2	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL port speed normal	normal	Port speed now above lower bound threshold.	102	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL port operational	normal	Processor can now communicate with DSL modem chip set.	105	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL SN selftest fail	warning	Self test failure from an SN.	19	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL test clear	normal	Test over.	106	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL test start	normal	Test started by any means.	6	hot_xdsl.mib (Hotwire XDSL Interface)
Ethernet link down	major	—	2	MIB II (RFC 1213)
Ethernet link up	normal	—	3	MIB II (RFC 1213)
Non-supported MCC	major	AN in Slot *xx* has been installed in a chassis that cannot support one or more of its features.	21	hot_sys.mib (Hotwire system)
Remote injection failure	warning	Cannot inject filters to SN on port *N*.	10	hot_xdsl.mib (Hotwire XDSL Interface)
Remote injection incompatible	warning	Injection not supported by the SN.	9	hot_xdsl.mib (Hotwire XDSL Interface)
Selftest failure	minor	Sent if any portion of the AN's restart/selftest fails.	16	hot_sys.mib (Hotwire system)
SN device failure	major	Operating software detected an internal device failure. SN is still operating.	18	hot_xdsl.mib (Hotwire XDSL Interface)
SN fatal reset	major	Variable binding field contains device failure code.	20	hot_xdsl.mib (Hotwire XDSL Interface)
SN device mismatch	minor	SN on port *N* does not match device described in port configuration role.	7	hot_xdsl.mib (Hotwire XDSL Interface)
SN device mismatch clear	minor	SN on port *N* now matches device described in port configuration table.	107	hot_xdsl.mib (Hotwire XDSL Interface)

Table E-2. DSL Card Traps (3 of 3)

Event	Severity	Comment	Trap #	MIB
SN loss of power	minor	Card received “last gasp” message from SN, followed by a link down condition one minute later.	17	hot_xdsl.mib (Hotwire XDSL Interface)
SN selftest failure	minor	Failure of SN hardware. This trap is only sent if the hardware failure still allows sending traps.	19	hot_xdsl.mib (Hotwire XDSL Interface)
Warm start	warning	Power on reset.	1	MIB II (RFC 1213)

authenticationFailure Trap

The authenticationFailure trap can be selectively enabled for all configured communities that have traps enabled. If any communities have the generation of trap messages enabled, then the generation of authenticationFailure traps is determined by the state of the global authenticationFailure switch.

The IP source address contained in trap messages is always the address of the MCC card. The MCC sends the trap to the management system destinations configured on the MCC and uses its own IP address in the source field. The trap identifies both the chassis slot and the DSL card port. This value uses slot numbers 1,000 to 20,000 for Slots 1 to 20 and adds the interface number 0 for the card, 1 to 999 for an interface.

The following traps in the Hotwire XDSL Interface MIB are not applicable: 4, 104, 8, 9, 10, 11, 12, 13, 14, and 15.

Trap message appears on your NMS screen in a manner similar to the following:

Severity	Date/Time	Source	Message
Minor	July 14 0700	135.28.144.75	Paradyne: xDSL Margin Low Interface 1003

Source is the IP address of the MCC card, and, under **Message**, 1003 is the DSL card in Slot 1, Port 3.

IP Conservation

The primary function of the management domain is monitoring and configuring the network. To reduce the number of IP addresses needed, only the MCC card has an IP address available to the rest of the network. That is, only the 10BaseT (eth1) IP address of the MCC card is configurable. This means that the Network Access Provider (NAP) assigns and configures only one IP address per Hotwire chassis, not separate addresses for each card or Service Node.

The following are the addressing features.

- The MCC presents only one IP address to the NAP. The NAP will only have a single IP address assigned to the Hotwire chassis.
- NSP addresses per AN card or endpoint are not required.
- If you have Paradyne OpenLane, SNMP agents automatically send modified community strings with slot information. If you are using another NMS or MIB Browser, you must append the slot number to the community strings.

Management Domain Packet Walk-Through

This section discusses the management traffic flow through the DSL cards and the MCC card. Regardless of the technology (RADSL, MVL, ReachDSL, SDSL, IDSL, ATM, TDM SDSL, etc.), management data flow is the same. For more information about individual DSL cards, refer to the appropriate documents in the *Product-Related Documents* section, in *About This Guide*.

Two scenarios are presented below as examples of SNMP Get and Response packet walk-throughs for the following devices:

- MCC card
- DSL cards

SNMP to the MCC card

1. The NMS SNMP manager sends an SNMP **`get`** request to the MCC card with the correct community string.
2. The MCC card processes the request, checking the community string for a locator suffix.
3. When no locator string is found (no DSL card destination), the MCC card assumes it is the target and responds to the request with a **`get`** response.

SNMP to a DSL Card (AN)

1. The NMS SNMP manager sends a packet to the MCC card with the correct community string. The community string contains the locator string suffix indicating the DSL card to which this packet is sent.
2. The MCC sends the packet to the correct DSL card.
3. When the DSL card responds, the MCC card forwards the response over the Ethernet interface to the NMS SNMP manager using its IP address and the card's locator string.

Supported MIBs

The DSL system supports standard as well as Enterprise MIBs. Various configuration, status, and statistical data within the SNMP agent is accessible from the DCE Manager. The content of an SNMP agent's MIBs are defined by various Internet Request for Comments (RFC) documents.

An OpenLane MIB browser requires the operator to load and compile the appropriate MIBs into its database before it can manage the DSL network. For more information about OpenLane, see the *OpenLane SLM Administrator's Guide*.

The following sections provide brief descriptions about MIBs. Complete, up-to-date details about the content of all DSL MIBs are available on the Paradyne Web site at **www.paradyne.com**. Select *Support →Technical Information → MIBs.*

Standard MIBs

The Hotwire DSL system supports the following:

- RFC 1213 – MIB II
  - — System Group
  - — ICMP Group
  - — UDP Group
  - — Transmission Group
  - — SNMP Group
- RFC 1573 – Evolution of the Interfaces Group
- RFC 2037 – Entity MIB
- RFC 1643 – Ethernet

System Group

The system group objects are fully supported.

Interfaces Group

The evolution of interfaces group (RFC 1573 converted to SNMP v1) consists of an object indicating the number of interfaces supported by the unit and an interface table containing an entry for each interface.

Extension to the Interface Table

Additional objects are supported for the interface table. They are based on extensions to the Evolution of Interfaces Group of MIB II (RFC 1573).

IP Group

The IP group objects are supported by the MCC only, for all data paths configured to carry IP data; namely the Ethernet and backplane interfaces of the MCC. All objects in the IP Group are fully supported.

ICMP Group, MIB II

The ICMP Group objects are fully supported for all data paths carrying IP data; namely the Ethernet and backplane interfaces of the MCC and the backplane interface of each DSL card.

UDP Group, MIB II

The UDP Group objects are fully supported for all data paths carrying IP data; namely the Ethernet and backplane interfaces of the MCC and the backplane interface of each DSL card.

Transmission Group, MIB II

The Transmission Group objects are supported on the DSL, serial and Ethernet ports. However, these objects are not defined with MIB II but through other Internet-standard MIB definitions. Two Transmission Group objects are supported:

- enterprise (transmission 22) – The transmission object is supported on the DSL interfaces.
- dots (transmission 7) – This set of objects describes the Ethernet interfaces.

SNMP Group, MIB II

The SNMP Group objects that apply to a management agent are supported by the MCC and DSL cards.

Ethernet Interface MIB

Ethernet MIB is described in RFC 1643, Managed Objects for Ethernet-like interfaces.

The following objects of this MIB are supported for both the e1a interface and the proxy agent for the RADSL SNs.

- dot3StatsIndex
- AlignmentErrors
- FCSErrors

Entity MIB

The Entity MIB (RFC 2037) contains 5 groups.

Paradyne Enterprise MIBs

The Hotwire DSL system supports the following Hotwire DSL Enterprise MIBs:

- **Bridge MIB (hot_bridge.mib)** – Provides an RFC 1493 Bridge MIB modified to include VNID data.

  This MIB for the DSL Access Nodes is based on the standard Bridge MIB (RFC 1493 – Managed Objects for Bridges), and has been customized to match special features of the bridge including VNIDs. TDM SDSL cards are not supported since they operate at the physical layer.

  Current support for this MIB is:

  — pdndot1Base Group

  — pdndot1dTp: entity's state for transparent bridging

  — pdndot1dStatic: entity's state for destination address filtering

- **Device Control MIB** – Provides a uniform method of resetting DSL cards. Only one object from this MIB is supported: devHWControlReset.
- **Device Health and Status MIB (devHealthAndStatus.mib)** – Provides the results of a self-test and contains the following object: devSelfTestResults "result string" where each field reports a specific self-test result and colons are used as delimiters.

  — Test results are "P" = PASS or "F"= FAIL

  — RESET values = POW (power-on reset), SW (software reset) or EXT (external).

- **Diagnostics MIB (hot_diag.mib**) – Four objects from hot_diag.mib implement the configuration download features via SNMP.
- **Domain MIB (hot_domain.mib)** – This MIB specifies the Level 2 forwarding features of the AN, including VNID groupings and next hop router addresses.

- **Hotwire DHCP MIB (hot_dhcp.mib)** – Describes characteristics of the DHCP functions.
- **Hotwire System MIB (hot_sys.mib)** – Describes the special characteristics of the DSL and MCC cards.
- **Hotwire xDSL MIB (hot_xdsl.mib)** – Describes characteristics of the various DSL modems functions.
  - — The xDSL Interface MIB specifies xDSL objects needed to support both a central and remote xDSL interface. The MIB includes entries in the Status Table and the Configuration Table. Some entries in the status table dealing with remote statistics are provided by the SN via the LMC on a periodic basis (nominal 15-minute intervals) for DSL cards. TDM SDSL cards do not support LMC; the standalone TDM SDSL units contain an SNMP agent for management.
  - — If the AN does not receive a block of data for an interval, it does not increment its valid 15-minute count, and the statistics for 15-minute, 1-hour and 24-hour periods reflect this lack of valid data. For example, if during a 24-hour period, two consecutive 15-minute data blocks are lost followed by a valid block and a request to view the statistics, the valid interval counters display 1 for the 15-minute interval, 2 for the 1-hour interval, and 94 for the 24-hour interval.
- **Paradyne Device MIB (pdndce.mib)** – Describes Paradyne devices.
- **Security MIB (devSecurity.mib)** – SNMP security is configured on the MCC card. Use the Source Address Check screen to prevent unauthorized managers from browsing or configuring the Hotwire DSL network.
  - — SNMP community strings provide a generalized measure of security, but using the Source Address Check Screen to enable IP address security by entering the IP address of authorized managers provides a much higher and more specific level of security.
  - — When IP address security is enabled, the source address of *any* SNMP message to the MCC card (in either the management or service domain) is checked against the authorized list and dropped if there is no match. This prevents unauthorized access to the MCC and the chassis.

Network Management Components

Figure E-1 and Figure E-2 show the components of the network management domain for both the 8610/8810 DSLAM and the Hotwire 8620/8820 GranDSLAM. The router between the MCC 10BaseT interface and the NMS is optional. The MCC card provides consolidated management for the Hotwire DSL cards and Service Nodes from remote network management workstations by means of SNMP, Telnet, or by local access through its VT100-serial interface.

It is recommended that you use Paradyne's OpenLane to simplify the operation and management of very large networks. The Hotwire DSL cards and Hotwire Service Nodes provide features for the OpenLane to allow you to monitor and manage your network from a central point.

However, any SNMP-compliant management tool may be used.

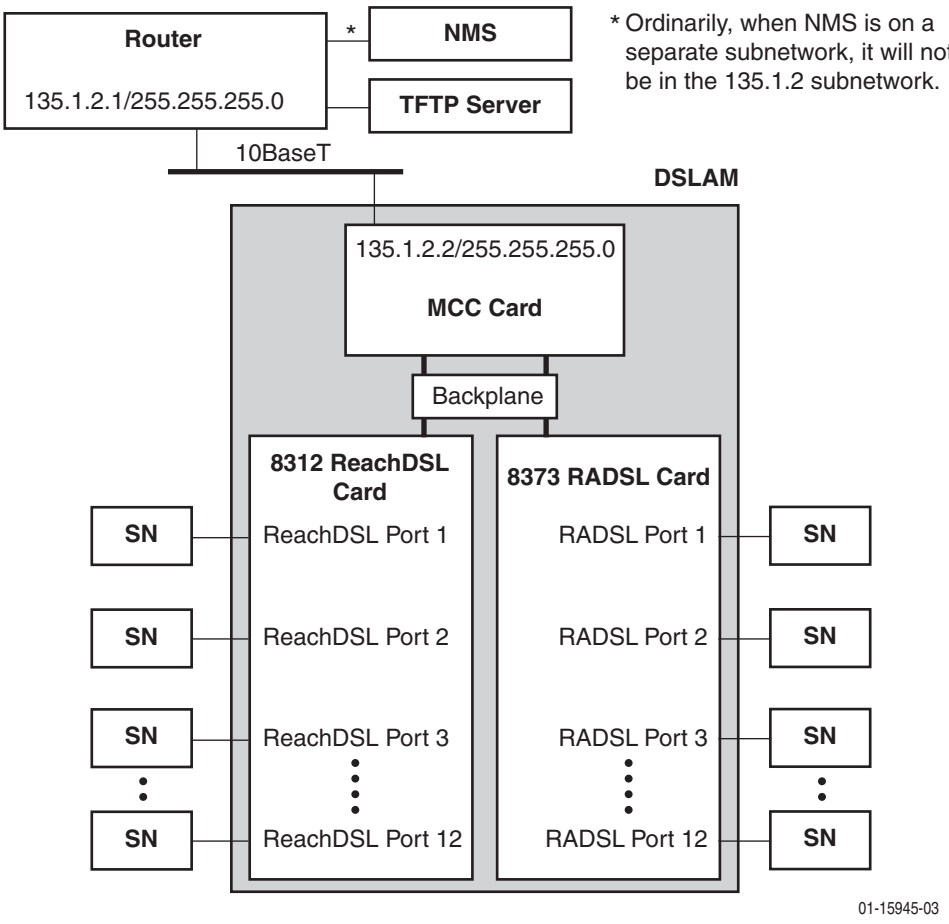


Figure E-1. Network Management Domain for 8610/8810 DSLAM Chassis

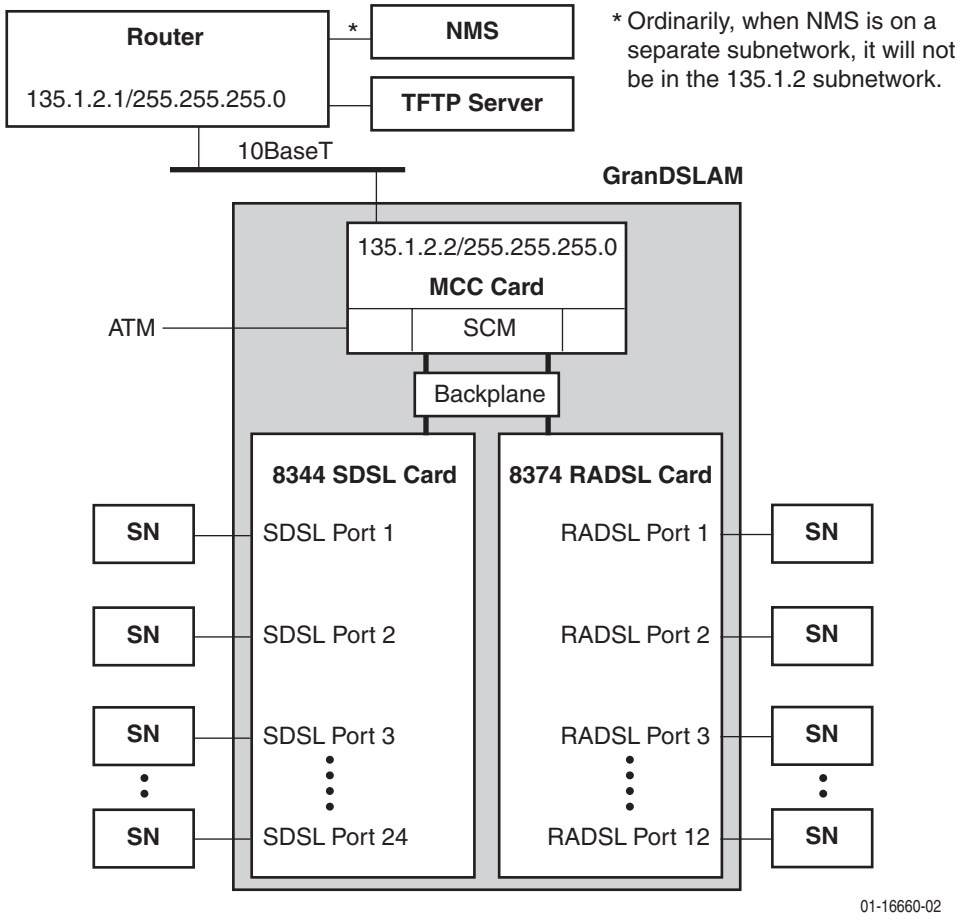


Figure E-2. Network Management Domain for Hotwire 8820 GranDSLAM Chassis

OpenLane Network Management Systems Overview

The OpenLane Service Level Management solution provides a method of monitoring, analyzing, and troubleshooting DSL devices through graphical user interfaces.

Features of OpenLane

OpenLane Service Level Management provides an integrated set of components used to administer, configure, monitor and diagnose Paradyne's Simple Network Management Protocol (SNMP) network access devices. It is available on Solaris systems or Windows NT.

The DSL system uses the MCC card in conjunction with OpenLane. The MCC card provides the single management interface to the Hotwire DSL cards and Service Nodes. The MCC card gathers operational status for each of the Hotwire DSL cards in the chassis and Service Nodes, and reports events and alarms to OpenLane.

This section lists only the OpenLane features that are applicable to the DSL devices. Use OpenLane to:

- Display performance graphs
- Create real-time Web-based performance reports
- Display Web health & status
- Monitor and troubleshoot devices and device interfaces
  - — Use color-coded icons to report the status of devices and device interfaces
  - — Obtain operational and administrative status on a device
  - — Identify the type of device, version number, release number, and more

For more information, see the appropriate OpenLane documentation available at **www.paradyne.com**. Select *OpenLane Network Management Solutions*.

SNMP Configuration Worksheets

This section provides worksheets to assist you in setting up general SNMP configurations for the MCC card on your Hotwire DSL network, such as defining communities, enabling traps, and preventing unauthorized access to the DSL system. These procedures provide minimal security. For additional security, be sure that source validation is enabled. Use the worksheets to record SNMP configuration parameters such as community names and IP addresses for associated SNMP NMS managers for a specific card. After the worksheets are completed, configure the SNMP agent via the Hotwire DSL user interface.

Summary: Configuring the SNMP Agent

In summary, to configure the SNMP agent:

- On the SNMP Communities/Traps screen, do the following:
  - — Assign an SNMP NMS manager to a community by specifying the SNMP NMS manager's IP address to a community name.
  - — Configure generation of all trap messages (except Authentication Failure Trap messages, which can be enabled or disabled independently).
  - — Enable or disable Authentication Failure trap messages.
- On the SNMP Security screen, you can enter the IP addresses of specific, approved SNMP NMS managers to prevent other managers from browsing the network. Use this screen to prevent unauthorized access to the DSL system.

Worksheet: Defining a Community and Enabling Traps

On the SNMP Communities/Traps screen, define a community by specifying the SNMP NMS manager who receives traps. Up to three managers can be assigned for each community. You can also enable or disable the generation of traps.

Access the . . .	By . . .
SNMP Communities/Traps screen	Selecting *Configuration* → *SNMP* → *Communities/Traps* (**A-F-A**) from the MCC menu.

SNMP Communities/Traps	
Prompt	**Your Configuration Setting**
1. Determine whether you want to enable or disable Authentication Failure traps: – Enter **enable** at the **`Enable/Disable:`** prompt to forward authentication failure traps to all SNMP NMS managers assigned to a community name. – Enter **disable** at the **`Enable/Disable:`** prompt to prevent the forwarding of authentication failure traps to all SNMP NMS managers assigned to a community name.	Authentication Failure Trap =
2. Change the default community names at the **`Community Name:`** prompt if desired. Hotwire DSL provides the following default community names: – **public** (RO – Read-Only) – **mcc** (RW – Read/Write) – **nms** (RW – Read/Write) – **nms - 2** (RO – Read-Only) You can change access permission for these communities. At the **`ReadOnly (ro)/ReadWrite (rw)/NoAccess (na):`** prompt, specify the desired permission for each community. **NOTE:** Make sure the SNMP NMS manager knows the correct community name. It needs the correct permission to access/browse the Hotwire DSL system.	Record the Community Names (default or new names) and their access permissions. **public** or _____ Access permission = **mcc** or _____ Access permission = **nms** or _____ Access permission = **nms – 2** or _____ Access permission =

SNMP Communities/Traps *(Continued)*	
Prompt	**Your Configuration Setting**
3. For each community name, you can enter IP addresses of up to three SNMP NMS managers. – At the **`(nnn.nnn.nnn.nnn):`** prompt, enter the IP addresses of the SNMP NMS managers. – At the **`Input Number`** prompt, enter the port number for each SNMP NMS manager specified. All traps go to the specified port. – At the **`Enable/Disable:`** prompt, indicate whether you want to enable or disable traps. Enter **E** to enable traps. This forwards traps to the specified SNMP NMS manager. Enter **D** to disable traps. This prevents the forwarding of traps.	**public** (RO) or _____: ■ IP address = Port = Forward traps (E or D) = ■ IP address = Port = Forward traps (E or D) = ■ IP address = Port = Forward traps (E or D) = **mcc** (RW) or _____: ■ IP address = Port = Forward traps (E or D) = ■ IP address = Port = Forward traps (E or D) = ■ IP address = Port = Forward traps (E or D) = **nms** (RW) or _____: ■ IP address = Port = Forward traps (E or D) = ■ IP address = Port = Forward traps (E or D) = ■ IP address = Port = Forward traps (E or D) = **nms – 2** (RO) or _____: ■ IP address = Port = Forward traps (E or D) = ■ IP address = Port = Forward traps (E or D) = ■ IP address = Port = Forward traps (E or D) =

SNMP Communities/Traps *(Continued)*	
Prompt	**Your Configuration Setting**
4. Press Ctrl-z and the **`Configuration has been modified. Save (yes/no)`** prompt appears. You have established Authentication Failure Trap security on the MCC. Repeat the procedure to create different levels of security for other IP addresses within the same community string or for other community strings.	Enter **yes** to save the configuration, **no** to delete the information.

Worksheet: Preventing Unauthorized Access

Use the SNMP Security screen to enable SNMP security (i.e., prevent unauthorized browsing or configuration of the Hotwire DSL network).

- If you want address security, activated it on the MCC and all DSL cards.
- If the NSP allows access to a limited set of DSL cards, that NMS's IP address should only be entered on those DSL cards in the limited set.

NOTE:

To completely disable SNMP access, do one of the following:

— Set the IP Address Security field to enable and do not enter any IP addresses on the screen, or

— Set the IP Address Security field to enable and make sure that the IP addresses entered on the screen are set to No Access.

SNMP Security	
Prompt	**Your Configuration Setting**
1. Determine whether you want to enable or disable Telnet Access Security Check: – Enter **enable** at the **`Enable/Disable:`** prompt to enable Telnet Access Security Check. – Enter **disable** at the **`Enable/Disable:`** prompt to disable Telnet Access Security Check.	Telnet Access Security Check =
2. Determine whether you want to enable or disable SNMP Access Security Check: – Enter **enable** at the **`Enable/Disable:`** prompt to enable SNMP Access Security Check. – Enter **disable** at the **`Enable/Disable:`** prompt to disable SNMP Access Security Check.	SNMP Access Security Check =
3. Determine whether you want to enable or disable FTP Access Security Check: – Enter **enable** at the **`Enable/Disable:`** prompt to enable FTP Access Security Check. – Enter **disable** at the **`Enable/Disable:`** prompt to disable FTP Access Security Check.	FTP Access Security Check =

Index

Numerics

10BaseT/100BaseT interface on the MCC card (eth1), 3-1

A

access
    firmware files, A-3
    levels, 1-4, 4-20
    security options, 4-24
accessing
    Hotwire - MCC Menu, 2-7
accessing the system for the first time, 3-4
Active Interfaces List screen, 5-11
Active Ports List screen, 5-7
Active sockets, 5-14
Add ARP Entry screen, 4-31
adding
    filters, 4-29
    static routes, 4-27–4-28
    users, 4-19
Address Resolution Protocol (ARP)
    adding cache parameters, 4-31
Administrator access permission, 1-4, 4-20
alarm indication, 1-3
alarms
    checking, 8-2
    major, 8-3
    minor, 8-4
Alarms screen, 7-3
Apply Download screen, 4-12
ARP Parameters screen, 4-35
ARP Table screen, 5-28
Asynchronous Terminal Interface (ATI), 1-3
ATM cards, 1-2
audience, vii
auto backup, 4-47
Auto Code Download, 4-48, A-12
auto restore, 4-47
automatic firmware download, 4-48, A-12
automatically logging off, 2-14

B

basic card information, 4-4
basic configuration tasks
    summary of, 3-6
    Task 2 - Creating SNMP Community Strings and Enabling Authentication Failure Traps, 3-7
    Task 3 - Creating the Default Route, 3-6
binding a filter, B-7
bringing down interfaces, 4-17
bringing up interfaces, 4-17

C

Card Info screen, 4-9
card reset, 4-7, 4-11
Card Reset screen, 4-7
Card Status Menu, 5-2
    Card Info, 4-4
    Card Reset, 4-7
    description, 4-3, 4-13, 4-44–4-45
    DNS Setup, 4-4
    Download Code, 4-8
    NVRAM Clear, 4-5
    NVRAM Config Loader, 4-6
    Time/Date, 4-5
changing
    filters, 4-29
    MTU value, 4-15
    users, 4-19
Chassis Info, 2-5, 2-13
Chassis Information screen, 2-13
checking alarms, 8-2
clearing NVRAM, 4-5
Communities/Traps screen, 4-38
community structures, E-2
components
    of a menu, 2-1
    of a screen, 2-2
config error, 8-4
Configuration Backup/Restore, 4-49
Configuration Menu, 2-11
    Access Security, 4-19
    Card Status, 4-3, 4-45
    DSL Cards, 4-39
    Files, 4-45
    Interfaces, 4-14
    IP Router, 4-26
    Ports, 4-13
    Slot, 4-39
    SNMP, 4-36
    Syslog, 4-44

configuration option tables
Access Security Menu, 4-24
Card Status Menu, 4-8
Interfaces Menu, 4-18
Slot (DSL Cards) Menu, 4-42
SNMP Menu, 4-38
summary, 4-2
configuration worksheets
filtering configuration, B-3
SNMP configuration, E-16
Configure Account screen, 4-20–4-22
Configure DNS screen, 4-4, 4-9
Configure User Accounts screen, 4-24
configuring
ARP parameters, 4-31
basic card-level information, 4-4
DNS servers, 4-4
DSL cards and Service Nodes (SNs), 8-2
filters, 4-29
IP addresses for the LAN port, 4-16
static routes, 4-27–4-28
Control Interface screen, 4-17–4-18
Control screen, 4-18
Current Users, 2-5
screen, 2-13

D

defining
a community, E-17
a filter, B-3
mappings between IP addresses and host names, 4-32
deleting
filters, 4-29
static routes, 4-27–4-28
users, 4-19
device and test monitoring, 1-3
diagnostics, 1-3, 1-6
Diagnostics Menu, 7-1
Alarm, 7-3
Selftest, 7-2
display area, 2-2
displaying
active interfaces, 5-11
active ports, 5-7
additional interface status information, 5-12
ARP table information, 5-28
Ethernet statistics, 5-8
filter information, 4-28–4-30
filters, 5-29
general card information, 5-3
IP statistics, 5-20
login history, 5-4
routing table statistics, 5-26
SNMP authentication statistics, 5-24
SNMP statistics, 5-22
socket statistics, 5-14
system errors, 5-5
TCP connection statistics, 5-19
TCP data statistics, 5-17
UDP statistics, 5-16
DNS setup, 4-4, 4-32
document summary, viii
Domain types, 3-2
Management domain, 3-2
Service domain, 3-2
Download Code screen, 4-12, A-5
Download screen, 4-8
downloading
code, 4-8
configuration data, 4-8
DSL card
reset slot, 4-40
DSL Cards Menu
description, 4-39
IDSL Card Setup, 4-41, 4-46
Reset Slot, 4-40
DSLAM
supported MIBs, E-9, E-11

E

editing
filters, 4-29
passwords and privileges, 4-19
enabling SNMP traps, E-17
entering card information, 4-4
eth1 interface, 3-1
Ethernet Port screen, 4-13
Ethernet Statistics screen, 5-9
displaying LAN port statistics, 5-8
exiting from a login session, 2-5, 2-14

F

failure
processor failure, 8-3
selftest failure, 8-3
use Ping screen, 8-5
use Telnet screen, 8-5
features, 1-1, 1-3
File System screen, 4-48
filter
adding, 4-29
binding a filter, B-7
changing, 4-29
configuration worksheets, B-3
defining a filter and rules, B-3
deleting, 4-29
description, B-1
displaying information, 4-28–4-30
maximum, 4-28–4-29
rule types, B-2
types of filters, B-1
Filter Table screen, 4-29, 5-29
firmware
file access, A-3
upgrade procedure, A-5
upgrade procedures, A-4
upload procedure, A-8–A-9
Flash File System, 4-48, A-7
Flash File System screen, A-9
FTP Server, 5-31

G

General Card Information screen, 5-3
General screen, 4-18

H

host address rule type, B-2
Host Table screen, 4-35
Hotwire - MCC Menu, 2-7, 2-10
Configuration Menu, 2-11
Monitoring Menu, 2-12
Hotwire Chassis Main Menu, 2-5

I

IDSL card, 1-2
clock setup, 4-41
IDSL Clock Configuration screen, 4-43
inband management, 4-13
initializing NVRAM, 4-5
input filter, B-1
interface information, 4-15
interface naming convention, 3-1
Interface Status screen, 5-12
interfaces
bringing down, 4-17
bringing up, 4-17
testing, 4-17
Interfaces Menu, 5-10
Control Interface, 4-17, 4-19
description, 4-14
General, 4-15
IP Network, 4-16
Interfaces screen, 4-15, 4-18
intranetworking communication problems, 8-5
IP address
configuring for LAN port, 4-16
in management domain, 4-16
managing, 4-32
mapping address and host name, 4-32
IP conservation, E-8
IP Filter Configuration screen, 4-34–4-35
IP Host Table screen, 4-32, 4-35
IP Network screen, 4-16, 4-18
IP Router Filters screen, 4-34–4-35
IP Router Menu, 5-25
ARP, 4-31
ARP Table, 5-28
description, 4-26
Filter Table, 4-29, 5-29
Host Table, 4-32
Routing Table, 5-26
Static Routes, 4-27–4-28
IP Routing Table screen, 5-26
IP Statistics screen, 5-20

L

LAN port
configuring IP addresses, 4-16
letter navigation keys, 2-1
levels of diagnostic/administrative access, 1-4
logging out, 2-5, 2-14
login session
exiting, 2-5, 2-14

M

major alarms, 8-3
Managed SN Select screen, 2-5–2-6
management domain
basic configuration, 3-6
components, 3-3, E-13
network management, E-13
packet walk-through (8546 DSL card), E-8
managing IP addresses and host names, 4-32
manually logging off, 2-14
Martian Networks screen, 4-33

MCC card
entering card information, 4-4
features, 1-1, 1-3
reset, 4-7
software functionality, 1-5
summary of basic configuration, 3-6
menu
components, 2-1
format, 2-1
list, 2-1
title, 2-1
menus
a hierarchical view, 2-5
Card Status, 5-2
Card Status Menu, 4-3, 4-13, 4-44–4-45
Configuration Menu, 4-1
DSL Cards Menu, 4-39
Interfaces, 5-10
Interfaces Menu, 4-14
IP Router, 5-25
IP Router Menu, 4-26
Monitor Servers, 5-30
Network Protocol, 5-13
Physical Layer, 5-6
Slot Menu, 4-39
SNMP Menu, 4-36
Users Menu, 4-19
Mgmt Card Select, 2-5
screen, 2-6
MIB compliance, E-9
minor alarms, 8-4
modem, remote access, D-1
monitoring
an interface, 4-17
device and test, 1-3
Monitoring Menu, 2-12
Card Status, 5-2
Files, 5-32
Interfaces, 5-10
IP Router, 5-25
Network Protocol, 5-13
Physical Layer, 5-6
Servers, 5-30
MVL cards, 1-1

N

navigation keys, 2-3
network
address rule type, B-2
interface options, 4-18, 4-38
intranetworking communication problems, 8-5
Network Management System (NMS), E-1
network model
management domain components, E-13
Network Protocol Menu, 5-13
IP Statistics, 5-20
SNMP Authentication Statistics, 5-24
SNMP Statistics, 5-22
Socket Statistics, 5-14
TCP Connection Statistics, 5-19
TCP Data Statistics, 5-17
UDP Statistics, 5-16
Network Protocol screen
SNMP statistics, 5-22
TCP statistics, 5-17
Network Time Protocol (NTP) server, 4-5
non-volatile database storage, 1-3
NVRAM clear out, 4-5
NVRAM Clear screen, 4-5, 4-10
NVRAM Config Loader screen, 4-6, 4-11

O

obtain interface information, 4-15
OpenLane, E-13
features, E-15
operator access permission, 1-4, 4-20
Operator Login screen, 2-4
organization of document, viii
output filter, B-1

P

passwords
adding, 4-19
editing, 4-19
Physical Layer Menu, 5-6
Port Card Select, 2-5
screen, 2-6
preventing unauthorized access, E-20
processor failure, 8-3
product-related documents, ix
purpose of document, vii

Q

Quick Card Select, 2-5
screen, 2-6

R

RADSL cards, 1-1
ReachDSL cards, 1-2
remote access through modem, D-1
Reset DSL Slot screen, 4-40, 4-42
resetting
DSL card, 4-40
MCC card, 4-7
restarting an interface, 4-17
resynchronization of backup files, 4-46
Routing Table screen, 5-26

rule types
host address, B-2
network address, B-2
socket address, B-2

S

screen
components, 2-2
format, 2-1
SDSL cards, 1-2
Selftest Results screen, 7-2
config error, 8-4
Servers Menu, 5-30
setting the time and date, 4-5
setup instructions, 3-1
SHDSL cards, 1-2
Simple Network Management Protocol (SNMP), E-1
Slot Menu
description, 4-39
SNMP
Authentication Statistics screen, 5-24
Communities/Traps screen, 4-38
community structures, E-2
configuration worksheets, E-16
management systems, 1-3
network management components, E-13
Sets, E-3
statistics, 5-22
traps, E-17
SNMP agent
configuration summary, E-16
defining a community, E-17
enabling traps, E-17
overview, E-1
preventing unauthorized access, E-20
SNMP Menu description, 4-36
SNMP Statistics screen, 5-22
socket address rule type, B-2
Socket Statistics screen, 5-14
software functionality
configuring the card, 1-5
monitoring the card, 1-6
troubleshooting and diagnostics, 1-6
starting an interface, 4-17
static routes
adding, 4-27–4-28
deleting, 4-27–4-28
maximum, 4-27
warning messages, 4-28
Static Routes screen, 4-27–4-28, 4-33
statistics
ARP table, 5-28
Ethernet, 5-8
IP, 5-20
routing table, 5-26
SNMP, 5-22
SNMP authentication, 5-24
socket, 5-14
TCP connection, 5-19
TCP data, 5-17
UDP, 5-16
status
codes, 2-7, 2-9
line, 2-2
stopping an interface, 4-17
summary of
basic configuration, 3-6
filter configuration, B-3
general SNMP agent configuration, E-16
supported MIBs, E-9, E-11
synchronizing the DSLAM's clock, 4-5
syslog, 5-5, 8-2
screen, 4-44
system header line, 2-2
System Information screen, 4-4
SYSYLOG, 4-44

T

TCP Connection Statistics screen, 5-19
TCP Data Statistics screen, 5-17
TCP statistics, 5-17
TDM SDSL cards, 1-2
testing interfaces, 4-17
TFTP server, 5-31
downloading from, 4-8, A-5
uploading to, 4-6
Time/Date screen, 4-5, 4-10
Traps, C-1
troubleshooting, 1-6
checking alarms, 8-3
configuration corruption, 8-4
Ethernet port failure, 8-3
fan alarm, 8-3
network problems, 8-5
Nonsupported chassis, 8-3
processor failure, 8-3
Selftest failure, 8-3
status codes, 8-1

U

UDP Statistics screen, 5-16
uploading configuration data, 4-6
User Accounts screen, 4-24

Users Menu
    Accounts, 4-20–4-22
    description, 4-19
using
    ARP submenu options, 4-31

W

warning messages for static routes, 4-28
Who Am I screen, 3-4–3-5